UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE QUITO

CARRERA:

INGENIERÍA DE SISTEMAS

Trabajo de titulación previo a la obtención del título de

Ingeniero de Sistemas

TEMA:

ANÁLISIS Y DISEÑO DE UNA PROPUESTA PARA MITIGAR ATAQUES CIBERNÉTICOS A CORREOS ELECTRÓNICOS UTILIZANDO TÉCNICAS DE HACKING ÉTICO

AUTOR:

FRANCISCO XAVIER ALVEAR REINOSO

TUTOR:

DANIEL GIOVANNY DÍAZ ORTIZ

Quito, febrero de 2019

CESIÓN DE DERECHOS DE AUTOR

Yo, FRANCISCO XAVIER ALVEAR REINOSO, con documento de identificación Nro. 1724484405, manifiesto mi voluntad y cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor del trabajo de titulación con el tema: ANÁLISIS Y DISEÑO DE UNA PROPUESTA PARA MITIGAR ATAQUES CIBERNÉTICOS A CORREOS ELECTRÓNICOS UTILIZANDO TÉCNICAS DE HACKING ÉTICO, mismo que ha sido desarrollado para optar por el título de INGENIERO DE SISTEMAS en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la Ley de Propiedad Intelectual, en mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia, suscribo este documento en el momento que hago la entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Politécnica Salesiana.

.....

FRANCISCO XAVIER ALVEAR REINOSO

CI. 1724484405

Quito, febrero de 2019

DECLARATORIA DE COAUTORÍA DEL TUTOR

Yo, Ing. DANIEL GIOVANNY DÍAZ ORTIZ, con documento de identificación Nro. 1716975501, declaro que bajo mi dirección y asesoría fue desarrollado el trabajo de titulación, con el tema: ANÁLISIS Y DISEÑO DE UNA PROPUESTA PARA MITIGAR ATAQUES CIBERNÉTICOS A CORREOS ELECTRÓNICOS UTILIZANDO TÉCNICAS DE HACKING ÉTICO, realizado por Francisco Xavier Alvear Reinoso, obteniendo un producto que cumple con todos los requisitos estipulados por la Universidad Politécnica Salesiana, para ser considerados como trabajo final de titulación.

Quito, febrero de 2019

.....

DANIEL GIOVANNY DÍAZ ORTIZ

CI. 1716975501

DEDICATORIA

A mis padres, Fausto y Susana, por ser el pilar fundamental que me ha permitido llegar a terminar mi carrera y lograr obtener un título universitario, por la paciencia, motivación y por ser ejemplo de disciplina y estudio ya que gracias a ellos terminé esta etapa de formación persona y profesional.

A mi hermana Carolina, por estar conmigo siempre y apoyarme incondicionalmente.

A mi novia Solange, que ha estado en los buenos y malos momentos en mi vida y siempre apoyándome para salir adelante y terminar todo lo que me propuse.

A mis amigos, que estaban pendientes de la culminación de todos mis propósitos, siempre dándome palabras de aliento para finalizarlos de la mejor manera.

¡Que nadie se quede afuera, se los dedico a todos!

Francisco Xavier Alvear Reinoso

AGRADECIMIENTO

Agradezco a los docentes de la Universidad Politécnica Salesiana, por haber compartido sus conocimientos y consejos para la vida profesional y de manera especial al Ingeniero Daniel Díaz por su amistad, por sus conocimientos y tiempo dedicado para acompañar el desarrollo de este trabajo y de esta manera culminar mis estudios universitarios.

Agradezco a mis padres por la dedicación, paciencia, esfuerzo y sabiduría que me han dado en mi vida y a lo largo de mi carrera universitaria.

A mi gran amigo Andrés, por ser un apoyo condicional desde el colegio hasta la vida profesional, por darme palabras de apoyo para seguir adelante y siempre confiar en mi capacidad de cumplir mis metas.

Un agradecimiento a ti Solange, mi compañera en mi vida universitaria, de trabajo de titulación y de vida.

Y a todas aquellas personas que de una u otra manera me apoyaron, me motivaron y ayudaron a culminar este objetivo personal.

Francisco Xavier Alvear Reinoso

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

Resumen

Los ataques a correos electrónicos han venido evolucionando con el paso de los años, estos ataques se han hecho más frecuentes y han causado daño a personas comunes y empresas con el robo del activo más importante que es la información, de esta manera se han desarrollado soluciones tanto de software como de capacitación para evitar que estos ataques cumplan con su objetivo.

El presente proyecto de titulación detalla los ataques a correos electrónicos y cuál es la información que el atacante necesita, para esto se define cada uno de los virus informáticos, gusanos y vulnerabilidades que aprovechan los hackers para poder ingresar al ordenador y realizar el ataque.

Basándose en casos reales, por medio de correo electrónico, se analizan los pasos que ha realizado el atacante hasta lograr su objetivo, también se analizan las soluciones que ofrecieron las empresas ante este tipo de eventos para que no vuelvan a tener un caso similar.

Por medio del Hacking Ético se realizan ataques de *spoofing*, *phishing*, *mailing* y correos híbridos con todos los ataques, de esta manera por medio de máquinas virtuales de *Amazon Web Service* se llega atacar a correos reales de 200 personas, para lograr una estadística mediante parámetros y de esta manera saber qué personas son más vulnerables y qué información concedieron al atacante.

Para esto, se plantea una solución de modo técnico y de capacitación para que las personas comunes o que están dentro de una empresa, no sean víctimas de ataques que tienen como objetivo el robo de información personal o financiera y el daño de la organización.

Abstract

Attacks on emails have been evolving over the years, these attacks have become more frequent and have caused harm to ordinary people and companies with the theft of the most important asset that is information, in this way, solutions have been developed as much of software as of training to avoid that these attacks fulfill their objective.

Based on real cases of attacks by email, it is analyzed all the processes that the attacker has to take to reach his goal, as well as the solutions offered by the companies, hoping not facing similar cases.

Through Ethical Hacking, spoofing attacks, phishing, mailing and hybrid emails are carried out with all the attacks, in this way through virtual machines (instances) of Amazon Web Services it is possible to attack real emails of 200 people, to achieve a statistic through parameters and in this way, to know which people are more vulnerable and what information was granted to the attacker.

To do so, a technical and training solution is proposed in a way that ordinary people or the ones into the company, won´t be the next victims of attacks that are aimed to stealing personal or financial information and damaging the organization.

INTRODUCCIÓN

Planteamiento del problema

Se habla de un ataque informático o ciberataque a un intento de una persona o grupo organizado, mediante el cual se infringe daños o modifica un sistema o red por varias razones. Dependiendo del tipo de ataque que se esté realizando, se pueden realizar con buenas intenciones para saber cuáles son las vulnerabilidades o con malas intenciones para poder obtener información importante, obtener dinero, entre otras y estos problemas puede llegar a destruir activos o información importante de una empresa.

Una de las características de realizar un ataque es que estos atacantes aprovechan alguna vulnerabilidad o debilidad del sistema informático, sistema operativo y hasta la persona que está ocupando este sistema para causar un efecto negativo en la seguridad informática.

Los equipos tanto de cómputo como equipos móviles llegan a infectarse por un software malicioso el mismo que en la mayoría de los casos llega a descargarse como un programa legítimo. Con un simple click se puede llegar a ejecutar este virus y el atacante llega a tener acceso total al dispositivo. Estos programas pueden ingresar a la computadora de diferentes maneras entre ellas por correo electrónico, por medio de descargas, ocultos dentro de otros programas y en la actualidad se han expuesto casos en los cuales al dar click sobre una imagen se ha ejecutado el programa.

Actualmente, este tipo de ataques ya representan el 70% de las amenazas informáticas que se producen en el mundo (POLICÍA NACIONAL DEL ECUADOR, 2018).

No siempre hace falta descargar el programa para que este infecte el computador, los atacantes buscan las vulnerabilidades del sistema para evitar que el usuario sepa que

se encuentra en un modo de ataque y están aprovechando estas vulnerabilidades para el robo de información.

Una de las preguntas que todos los usuarios se hacen es qué tan vulnerables son sus correos electrónicos para tener información crítica, esto depende de la seguridad que mantenga el servidor de correo que esté utilizando. Además, sin buenas políticas de correo corporativo es muy fácil tener muchas vulnerabilidades las mismas que van a ser aprovechadas por el atacante. (J.M.S., 2013).

Las empresas con servicio de correo gratuito como Google o Microsoft cada año invierten millones de dólares en seguridad para poder brindar un servicio excelente y que los usuarios sientan que su información está protegida contra cualquier problema o ataque tanto dentro de los servidores de estas plataformas como desde sus ordenadores.

Los atacantes para poder ingresar a un sistema informático o a correo electrónico utilizan programas de generación de claves las mismas que son ingresadas automáticamente a velocidades impresionantes, si la empresa no tiene una política de seguridad fuerte en la creación de claves para correo electrónico este programa podrá descifrar fácilmente la clave.

Para todos estos problemas en la red y sistemas existen programas o dispositivos que sirven para mantener la seguridad en un estado aceptable, uno de estos programas se denomina *honeypots* los mismos que están creados con el objetivo de atraer ataques de todo tipo para obtener información de los ataques simulando que es un computador con muchas vulnerabilidades, con esta información las personas encargadas de la seguridad de la red saben a dónde fue dirigido el ataque y qué pueden robar de este sistema o servidor.

Justificación

El ataque de virus informáticos se produce tanto al *hardware* como al *software* y al usuario final por lo que es imperativo que las personas y organizaciones dispongan de herramientas preventivas y disuasivas como: estar protegido por un servicio de antivirus para los computadores de la empresa y un antivirus específico para el servidor, esto ayuda a reducir la probabilidad que un virus, gusano o troyano ingrese; habilitar un *firewall* que tenga un control de las páginas que pueden o no ingresar y cerrar puertos por los cuales puedan ingresar al sistema; disponer políticas de seguridad de la información difundidas y de cumplimiento obligatorio; disponer de planes de contingencia debidamente validados.

El usuario debe evitar descargar programas de sitios que no son seguros ya que aquí es donde aprovechan los *hackers* para infectar el programa y al momento de instalarlo también correr su programa malicioso para lo cual la solución es bloquear estas páginas conocidas donde se pueden descargar programas infectados en su mayoría.

Las vulnerabilidades de sistema, en este caso el sistema operativo, se da por no actualizarlo, es aquí donde aprovechan los *hackers* como una puerta por la cual entrar en su computador y poder robar sus archivos o datos importantes.

Como idea principal se pretende ejecutar ataques a correos electrónicos y verificar sus vulnerabilidades con el propósito de establecer herramientas que permitan neutralizar el *hackeo* y, además, saber qué información se puede robar a través del correo electrónico y determinar el impacto en las personas y organizaciones por este tipo de piratería informática.

El trabajo tendrá como fundamento los principios de *Hacking* Ético y Ciberseguridad estudiados en la carrera y que encuentran su aplicación práctica en el mundo real.

Objetivo General:

Analizar y diseñar una propuesta para mitigar ataques cibernéticos a través de correos electrónicos utilizando técnicas de *hacking* ético.

Objetivos Específicos:

Analizar los diferentes tipos de ataque cibernético a correos electrónicos con el propósito de conocer qué información es la que buscan a través de este método de ataque.

Evaluar las soluciones existentes en la actualidad para mitigar los ataques realizados a los correos electrónicos y su nivel de efectividad.

Simular un servidor de correo electrónico con varios usuarios a los cuales se envía correos maliciosos determinando cuántos de ellos son víctimas de *hackeo* y poder así mitigar el proceso de una manera eficiente y rápida.

Realizar pruebas en las cuales se obtenga un porcentaje considerable de ataques mitigados mediante el empleo de herramientas de *hacking* ético.

Generar una propuesta de diseño de solución para mitigar los ataques cibernéticos realizados a los correos electrónicos de una manera efectiva antes que se roben información crítica.

Metodología de Investigación utilizada

Por el diseño de investigación se utilizaron dos tipos:

Investigación exploratoria para el análisis documental de las características que tienen los ataques cibernéticos, quiénes los provocan, qué efectos tienen en las organizaciones y los perjuicios que ocasionan

Investigación descriptiva, mediante la cual se registran los resultados que se obtienen del simulador del servidor de correo electrónico y sirve para el diseño de la propuesta de mitigación de ataques cibernéticos utilizando *hacking* ético.

La metodología se resume en la siguiente tabla:

Tabla 1 Comparativa de Metodologías Ágiles

	XP	SCRUM	CRYSTAL	MSF
CREADOR	Kent Beck	Jeff Sutherland, Ken Sch Waber	Alistair Cockbum	Microsoft
AÑO	1999	1995	1990	1994
CARACTE-RISTICAS	▪ Pequeñas mejoras, unas a otras ▪ Pruebas unitarias continuas ▪ Programación de tareas en parejas ▪ Corrección de todos los errores ▪ Propiedad del código compartida ▪ Simplicidad en el código	▪ Enfatiza valores y prácticas de gestión ▪ Hace usos de equipos ▪ Puede ser aplicado teóricamente ▪ Interacciones en orden de tiempo ▪ Se convoca diariamente para generar un avance	▪ Entregas frecuentes, en base a un ciclo de vida ▪ Mejora reflexiva ▪ Comunicación osmótica ▪ Seguridad Personal ▪ Fácil acceso a usuarios expertos ▪ Entorno técnico con pruebas automatizadas	▪ Es adaptable ▪ Es escalable ▪ Es flexible ▪ Modelo de Arquitectura del Proyecto ▪ Modelo de Equipo ▪ Modelo de Proceso ▪ Modelo de Gestión de Riesgo ▪ Modelo de Diseño de Proceso
ETAPAS	1.Planificación de proyectos 2. Diseño 3.Codificación 4. Pruebas	1.Planteamiento 2. Montaje 3. Desarrollo 4. Liberación	1. Entrega frecuente 2.Comunicación 3.Mejora Reflexiva 4.Seguridad Personal 5. Foco	1. Visión 2. Planificación 3. Desarrollo 4. Estabilización 5.Despliegue o implementación

			6. Fácil acceso a usuarios	

Nota: Comparativa de metodologías ágiles más utilizadas

Tabla 2 Comparativa de Metodologías Ágiles

CARACTERISTICAS	Pequeñas mejoras, unas a otras	Enfatiza valores y prácticas de gestión	Fácil acceso a usuarios expertos	Se convoca diariamente para generar un avance	Es adaptable	Es flexible	Programación de tareas en parejas
XP	x		x		x		x
SCRUM	x	x	x	x	x	x	
CRYSTAL		x		x	x		
MSF	x		x		x	x	

Nota: Características principales de las metodologías ágiles más utilizadas.

Mediante esta tabla comparativa de Metodologías Ágiles se llegó a la conclusión que la Metodología SCRUM es la que más ventajas presenta para el desarrollo de este proyecto de titulación, ya que se maneja interacciones en orden de tiempo y se generan avances diarios que facilitan el control de los resultados de la investigación.

CAPITULO 1

ESTADO DEL ARTE

1.1. Fundamentación Legal

La vertiginosa evolución de las tecnologías de la información y comunicaciones (TICS), así como de los sistemas de computación y electrónicos que se inventan cada día están impactando favorablemente en la calidad de vida de los seres humanos y favoreciendo el desarrollo de las empresas de todo tipo alrededor del mundo; igual, con la misma velocidad, los delincuentes han diseñado un sinnúmero de modalidades para vulnerar las seguridades de las redes y apropiarse de información sensible que les puede generar grandes réditos; a estas modalidades se da en llamar cibercrímenes y los estados del mundo se han visto obligados a la promulgación de leyes nacionales, transnacionales y el diseño de regulaciones y filtros para contrarrestar los ataques cibernéticos.

En el Ecuador el Código Orgánico Integral Penal, Art. 190: Apropiación fraudulenta por medios electrónicos.- establece que “La persona que utilice fraudulentamente un sistema informático o redes electrónicas y la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años. La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a

distancia, o violación de seguridades electrónicas, informáticas u otras semejantes". (Nacional, 2014)

El Artículo 232.- Ataque a la integridad de sistemas informáticos del COIP establece que "La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años." (Nacional, 2014)

El Artículo 229.- Revelación ilegal de base de datos, manifiesta que "La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años." (COIP, 2014).

La Ley Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, vigente, establece que: "Los mensajes de datos estarán sometidos a las leyes, reglamentos y acuerdos internacionales relativos a la propiedad intelectual", por lo tanto, protege al propietario de la información generada electrónicamente y que se graba en dispositivos de almacenamiento de datos.

Es en este entorno que el trabajo de un hacker ético cobra vital importancia, en la medida que debe identificar las vulnerabilidades de los activos antes de que los criminales lo hagan, anticipando acciones para neutralizar cualquier tipo de actividades maliciosas.

1.2. Fundamentación Teórico Conceptual

El Global Riks Report 2018 señala a los ciberataques y el robo de datos como dos de los riesgos más probables de que sucedan. Los ataques contra empresas casi se han duplicado en cinco años, y los incidentes que una vez se consideraron extraordinarios se están convirtiendo en algo común, explica el informe. Otra tendencia creciente es el uso de ataques cibernéticos para atacar infraestructuras críticas y sectores industriales estratégicos, lo que hace temer que, en el peor de los casos, los atacantes puedan desencadenar un colapso en los sistemas que mantienen funcionando a las sociedades. (Gray, 2018).

Bad Rabbit, NoptPetya, Wannacry. Estos tres *ransomware*, o programas dañinos, han paralizado cientos de miles de computadoras en todo el mundo y llenado los bolsillos de los *hackers*. *Wannacry*, que atacó en mayo de 2017 los servicios de salud británicos, las plantas del fabricante francés de automóviles Renault, los ferrocarriles alemanes y el gobierno español, habría generado 140 millones de dólares en ingresos a los extorsionadores.

Los piratas informáticos podrían dañar o destruir los objetivos en lugar de bloquearlos. Sus nuevas víctimas podrían ser adineradas personalidades a través de sus objetos conectados, menos seguros que las PC o los teléfonos inteligentes.

Los ataques que se encuentran comúnmente son: hackear una cuenta de Facebook el mismo que se oferta en las redes sociales por 91 euros, realizar el bloqueo de una página web dependiendo de qué tipo de página y dificultad tenga el costo esta entre 15 a 440 euros, descifrar un archivo encriptado puede llegar a costar apenas 40 euros tomando en cuenta la información que se encuentra dentro de este archivo sea de suma

importancia, en el mercado negro se puede llegar a encontrar muchos de estos servicios. (Ibáñez, 2015).

El origen de los ataques a computadores inicio en 1.949, por la vulnerabilidad de los incipientes sistemas informáticos, y desde esa fecha los piratas informáticos no han parado en sus intenciones de atacar los equipos, sin embargo, solo algunos -aunque cada vez en mayor número- generan alarma en el mundo entero por su capacidad de propagarse a través de las redes y causar daños de gran magnitud.

Los países con más ciberataques son Rusia, Taiwán, Alemania, Ucrania, Hungría, Estados Unidos, Rumanía, Brasil, Italia, Australia. (Tiempo, 2015)

Es necesario tener en cuenta dentro de la seguridad de correo electrónico como de servidores y del gran campo del *HACKING* ETICO algunas premisas básicas como el perfil del *Hacking* Ético, qué es una amenaza, vulnerabilidad, ataque, gusano, virus, spoofs, scanning y los diferentes tipos de ataque en contra de una red o de un correo electrónico, con el propósito de mantener un lenguaje común y la compresión similar, tanto del lector como del investigador.

1.2.1. Ciberseguridad

En un inicio, en el mundo de la ciberseguridad, a quienes se los denominaba delincuentes cibernéticos eran jóvenes que tenían un conocimiento amplio y mucha curiosidad en los sistemas a los que ingresaban desde la computadora de su hogar y sus ataques cibernéticos solo llegaban a ser bromas y vandalismo en páginas web.

En la actualidad es de conocimiento mundial que existe varios grupos de delincuentes cibernéticos los cuales se han hecho famosos en el mundo por sus diferentes tipos de ataque. Estas personas tienen un alto conocimiento de sistemas, pero, sobre todo, saben encontrar las vulnerabilidades de los sistemas informáticos, estos delincuentes

cibernéticos cuando pueden ingresar al sistema todo les sirve, empezando desde tarjetas de crédito, diseño de productos y sobre todo el activo más importante de una empresa que es la información. (Academy, 2018)

En este grupo se han podido identificar diferentes tipos de atacantes cibernéticos y se pueden clasificar en:

- **Aficionados o *script kiddies*:** Estas personas no tienen un conocimiento amplio sobre sistemas y en la mayoría de las ocasiones utilizan programas o tutoriales que se encuentran en la red, algunos de ellos logran su objetivo de una manera curiosa, pero otros con la utilización de estas herramientas logran su objetivo con el fin de demostrar sus habilidades y causar daño. Estas personas, no por no tener un amplio conocimiento, dejan de ser peligrosos, es más, pueden llegar a realizar un daño devastador.
- ***Hackers*:** Este grupo de atacantes cibernéticos son los más famosos en la sociedad por los daños que han causado en los sistemas, ellos ingresan a una computadora o a una red empresarial con varios motivos. La intención con la cual ingresan ha permitido crear una clasificación de estos atacantes como *hackers* de sombrero: blanco, gris y negro.
- Los atacantes de sombrero blanco son personas que ingresan a la red o a un sistema informático con el fin de descubrir las vulnerabilidades y así la empresa pueda mejorar la seguridad de estos sistemas, estos *hackers* obtienen las credenciales para poder interrumpir ciertos procesos del sistema y así obtener pruebas para generar un reporte de qué pasaría en el caso real de interrupción del sistema.
- Los *hackers* de sombrero negro son personas con alto conocimiento informático los mismos que ingresan a redes empresariales en busca de

ganancias ilícitas personales, financieras y en algunos países, son considerados los atacantes más peligrosos.

- Los *hackers* de sombrero gris pueden encontrar vulnerabilidades y señalarlas a las personas encargadas de la seguridad dentro de la empresa si su propósito es ese, caso contrario pueden exponer estas debilidades en internet para que otros *hackers* utilicen este recurso y puedan utilizarlo para su conveniencia, estos *hackers* son famosos por tener propósitos buenos o malos dependiendo de quién los contrate y sobre todo tienen fines económicos propios.
- ***Hackers* organizados:** Estos atacantes incluyen organizaciones de delincuentes informáticos, *hacktivistas*, terroristas y *hackers* patrocinados por el Estado. Las organizaciones de delincuentes informáticos tienen como objetivo realizar ataques a grandes empresas o gobiernos a quienes roban información para luego poder venderla u obtener beneficios personales, los *hacktivistas* se pueden clasificar en atacantes en contra del gobierno o atacantes a favor del gobierno para lo cual ellos realizan publicaciones embarazosas sobre sus víctimas, estos atacantes tienen auspiciantes los cuales quieren sacar beneficio de estas difamaciones, también utilizan información falsa para que el gobierno del cual están patrocinados sobresalga con una noticia que los beneficia, en algunos países estos atacantes son parte de su propio gobierno los cuales pueden ser grupos de inteligencia formados en la policía o militares.

1.2.1.1. Medidas de seguridad ante atacantes cibernéticos.

Frenar los ataques cibernéticos es una tarea muy difícil ya que los atacantes están siempre pendientes de las mejoras tecnológicas y cómo poder vulnerarlas o utilizarlas en su beneficio. Sin embargo, las empresas, gobiernos y organizaciones han tenido que

tomar precauciones para poder contener los numerosos ataques, estas son algunas de las acciones:

- La *Common Vulnerabilities and Exposures* (CVE) que es la base de datos Vulnerabilidades y Exposiciones Comunes es una de las herramientas más utilizadas para poder contrarrestar los ataques teniendo así en las manos una base actualizada y retroalimentada de varias organizaciones las mismas que comparten entre sí información importante para mantenerse alejados de muchos de los ataques más comunes.
- El establecimiento de sensores de advertencia ante posibles ataques es otra de las maneras más efectivas de poder disuadir con tiempo un ataque externo, para ello se mantienen supervisados los equipos que tienen información crítica o se crea un objetivo propenso a ataques el mismo que advierte de los ataques potenciales al objetivo verdadero.
- Los gobiernos en su mayoría tienen un departamento o agencia de inteligencia los mismos que se encuentran en constante desarrollo de fortalezas en contra de los ciberataques y estas agencias colaboran con esta información a empresas o gobiernos diferentes para poder evitar ataques similares en otros lugares.
- Regirse a buenas prácticas o a una certificación de calidad es fundamental para tener procedimientos sobre seguridad de la información, uno de los estándares más utilizados para esto es la ISO 27000 y esto da un avance a un estándar internacional de seguridad de la información en todo el mundo.

1.2.1.2. Amenazas de seguridad interna y externa

Las amenazas de seguridad de la información son el eje fundamental que tienen los expertos para saber cuáles son las vulnerabilidades que tienen los sistemas o personas. Las amenazas internas por muchos años siempre fueron malentendidas por los

expertos de la seguridad de la información, pero con el pasar de los años esta amenaza se ha convertido en la que mas daño ha realizado a las pequeñas y grandes empresas, haciendo a los usuarios una vulnerabilidad más para la empresa.

De este nuevo descubrimiento se han sacado aspectos positivos y negativos, ahora se da capacitaciones constantes a usuarios de sistemas que contiene información crítica, pero aun es preocupante los incidentes que se dan por medio de esta amenaza.

Amenaza de seguridad interna y externa

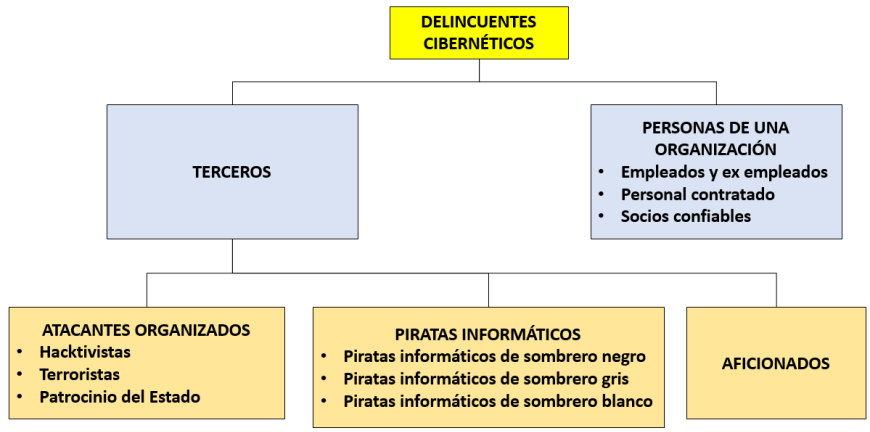

Figura 1 Seguridad interna y externa
Elaborado: Francisco Alvear

1.2.1.2.1. Amenazas de seguridad interna

Los empleados internos de una organización tienen más potencial de poder robar información, así como ejecutar programas con virus descargados como archivos adjuntos de los correos electrónicos, las personas que atacan una red internamente son personas con alto conocimiento de cómo funciona la red y sus recursos, además tienen acceso con claves a servidores y a datos críticos dentro de la empresa así que por estas razones los hace mucho más peligrosos que los atacantes externos.

Un empleado interno, un usuario invitado o un proveedor de servicios puede, de una manera accidental, intencional o con fines maliciosos ingresar a su computador un malware por medio de un correo electrónico o una página web no segura; facilitar a personas externas ingresar USB infectadas con virus en los computadores de la organización o corromper la información de la empresa modificándola, eliminándola o cambiando datos.

Una de las medidas que toman las empresas contra estos ataques internos es exponer las políticas de seguridad de TI a todos sus empleados y cuáles son las repercusiones que tienen si no se dan cumplimiento a las mismas.

1.2.1.2.2. Amenazas de seguridad externa

Los atacantes externos son personas aficionadas o con altos conocimientos de las vulnerabilidades que pueden tener los sistemas informáticos y redes corporativas para explotar la información que tienen estas empresas. Los datos más preciados para estas personas incluyen información personal y datos financieros. Estos datos personales pueden contener información crítica como números de cedula, seguro social o cualquier información importante que puede ser utilizada para tomar decisiones de empleo. En los datos financieros pueden encontrar información como: declaración de ingresos, balances, declaraciones de flujos. Estos documentos dan información del estado financiero de la empresa.

1.2.1.3. Vulnerabilidades de los dispositivos móviles

En el pasado las empresas disponían de un ordenador de escritorio y lo delegaban a una persona a cargo la misma que ingresaba junto a su cuenta y sus datos personales en un servidor de directorio activo el mismo que controlaba a todas estas máquinas ya que estaban conectadas a la red vía *Ethernet*. El personal de sistemas siempre estaba

pendiente de que los sistemas operativos y requisitos de seguridad estén al día para así tener vulnerabilidades dentro de los equipos de la empresa. En la actualidad se sigue usando este tipo de dispositivos, pero con la utilización de *Smartphone, IPhone, tablets* y *laptops* personales han ido destituyendo a los computadores de escritorio, el personal de la empresa utiliza estos dispositivos para tener acceso a la información de la empresa y sobre todo estar siempre en línea mediante el correo electrónico y plataformas interactivas de documentos e información. *Bring Your Own Device* (Trae tu propio dispositivo) esta tendencia en crecimiento dentro de las empresas ya que así pueden llevar sus documentos, programas y trabajo a casa. Uno de los mayores problemas que se tiene es el control de estos dispositivos móviles ya que pueden tener sistemas operativos ilegales, virus dentro de su PC, antivirus caducados y más problemas que tiene un dispositivo personal.

1.2.1.4. Servidor DNS

Un servidor DNS es un Sistema de Nombres de Dominio el mismo que se encarga de traducir la dirección IP a un nombre de dominio y viceversa. Las redes TCP/IP se comunican mediante direcciones IP cada PC tiene una dirección IP asignada y es por esta dirección que puede comunicarse con las demás PC en la red.

Para los usuarios trabajar con direcciones IP en los navegadores sería una tarea muy difícil y tediosa ya que tendrían que aprenderse una serie de números para poder conectarse a cualquier página web. En su lugar se utiliza el servidor DNS para poder navegar más fácilmente por la web ya que es más fácil utilizar un nombre que una serie de números como por ejemplo: www.google.com y no 172.217.22.142, este cambio es transparente para el usuario pero el proceso que se realiza es que nuestra PC o dispositivo conectado al Internet tendrá que averiguar cuál es la IP correspondiente a www.google.com y que así el servidor web podrá mostrar el contenido de la página

web, si en el navegador utilizamos directamente la IP 172.217.22.142 se ahorrará el paso de averiguar a qué dirección IP pertenece ese nombre. El servidor DNS puede realizar esta tarea con una base de datos extensa la misma que tiene todos estos nombres que pertenecen a una IP determinada, Google tiene también sus servidores DNS los cuales son muy prácticos ya que tiene una base de datos grande en la cual se encuentran todos los nombres pertenecientes a las direcciones IP. (Profesorado, s.f.).

1.2.2. Perfil del *Hacker* Ético

El *hacker* ético es un profesional de la seguridad de redes que está comprometido con el análisis de las vulnerabilidades y evaluación de las amenazas a los sistemas y programas informáticos corporativos de una organización para conocer el estado real de la seguridad, posee excelentes habilidades técnicas e informáticas, experiencia en computación y es muy confiable. Tiene como misiones fundamentales las siguientes:

- Actuar en forma proactiva e innovadora, adelantándose a los posibles cibercriminales solucionando vulnerabilidades en los sistemas que pueden provocar un ciberataque.
- Identificar los objetivos de los cibercriminales bajo las potenciales amenazas a la organización para tomar las medidas apropiadas que proveen una protección adecuada.
- Investigar si se han registrado actividades maliciosas y qué medidas preventivas se han tomado, para deducir el perfil indirecto de las habilidades del atacante.
- Concienciar a los profesionales de las organizaciones públicas y privadas sobre la importancia de la seguridad informática en su trabajo diario.

- Mejorar los procesos de seguridad en los sistemas y programas informáticos de la organización mediante acciones de actualización de software, plan de respuesta a incidentes, continuidad del negocio, entre otros.

Los principales valores de un hacker ético son: pasión por su trabajo, libertad, conciencia social altamente definida, lealtad, capacidad para trabajar en equipo y soportar la presión, anticorrupción, libre acceso a la información disponible en redes, accesibilidad, actividad, preocupación responsabilidad, curiosidad, creatividad, proactividad, interés, solidaridad e integridad.

1.2.3. Ataque a los sistemas de seguridad implementados.

Un ataque es un asalto a la seguridad del sistema que se deriva de una maniobra bien planeada; es cualquier acción que intenta violar la seguridad del sistema. (Gaibor, 2007). Los ataques siempre están en constante desarrollo ya que siempre se logra tener un plan de contingencia para mitigarlos, para ello los *hackers* están en constante desarrollo de nuevos ataques tomando en cuenta las vulnerabilidades que presentan los sistemas en los componentes de diseño, configuración y operación.

Existen dos tipos de ataques: los ataques activos y los ataques pasivos estos se denominan así dependiendo de los objetivos y efectos que pueden tener dentro del sistema.

Los ataques activos utilizan las vulnerabilidades para producir daños en un sistema, modificarlo o con el fin de obtener información confidencial de la empresa, este tipo de ataques son los más perjudiciales, pero son más fáciles de detectar ya que al momento que inicia el ataque empieza a tener fallas el sistema y así el administrador tiene conocimiento que un posible *hacker* quiere hacer daño o robar información de la

organización. Uno de los ataques activos que el mundo conoce es el DoS (*Denial of Service*), este ataque afecta la disponibilidad, integridad y autenticidad de un sistema.

Los ataques también dependen de quiénes los están realizando y pueden ser personas internas o externas dependiendo de lo que se quiere realizar, un ataque interno es realizado por una persona dentro de la organización que tiene el conocimiento para poder ingresar información confidencial quienes pueden desde dañar hasta robar información importante del sistema.

Un atacante externo es realizado por una persona no autorizada o ilegitima. Los principales atacantes externos son *hackers* con un conocimiento avanzado o un novato que quiere probar suerte al querer ingresar al sistema.

Los ataques pasivos son aquellos que se infiltran dentro de un sistema pero no se los detecta fácilmente sus funciones en la mayoría de los casos es aprender cómo está estructurada la red, quiénes son los usuarios que tienen más privilegios y sobre todo es el aprendizaje de las vulnerabilidades del sistema un ejemplo de un ataque pasivo es interferir en las transmisiones electrónicas para dar o dejar mensajes o para obtener contraseña inseguras, la confidencialidad dentro de los ataques pasivos juegan un papel muy importante para prevenir el descubrimiento de información por parte del personal no autorizado.

1.2.4. Tipos de Ataque

1.2.4.1. Ataques Informáticos

1.2.4.1.1. Malware

El termino malware es la abreviatura de software malicioso, este término conlleva a todos los códigos maliciosos y programas los cuales tienen como objetivo es dañar un

sistema o aprovechar sus vulnerabilidades para dañar archivos importantes del sistema operativo con el fin de causar un mal funcionamiento. (RIVERO, 2016)

Tomando en cuenta la definición de *malware* se tiene el siguiente ejemplo: en la plataforma más famosa para descargar aplicaciones en *Android Google Play* se encontraba un *malware* escondido durante 3 años, esta aplicación cuenta con más de 3 millones de descargas, el nombre de la aplicación es *System Update* la cual ha hecho que millones de usuarios inexpertos se la descarguen para poder actualizar su *Android,* la aplicación al momento de ejecutarla genera un error y se elimina de la pantalla del equipo quedando ejecutándose en segundo plano y convirtiéndose en un *Spyware* en tiempo real logrando así recopilar información importante de sus víctimas. (Collado, 2017).

1.2.4.1.2. Virus

Los virus informáticos son programas con un fin malicioso que tiene como objetivo replicarse y dañar otros archivos del sistema operativo con la intención de causar un daño o modificación para su mal funcionamiento.

Estos programas se encuentran dentro ejecutables de programas conocidos, al dar click sobre él se pueden replicar dentro del sistema operativo y ya que se han dañado archivos importantes del sistema este programa infecta unidades de almacenamiento con el fin expandirse por este medio a los demás ordenadores. (Rivero, 2018)

Uno de los virus más famosos se generó en los inicios del Internet cuando David L. Smith creó el virus llamado Melissa el mismo que llegaba vía correo electrónico como un documento de Word adjunto al correo con nombre “Acá está ese documento que me pediste, no se lo muestres a nadie más”. Al momento de ejecutar este documento desactivaba opciones de procesador de texto y cambiaba la extensión de los

documentos de texto. Su expansión por internet era incontrolable ya que utilizaba la libreta de direcciones de *Outlook* y se reenviaba a los primeros 50 contactos del usuario que lo ejecutaba. (Tercera, 2012).

1.2.4.1.3. Gusanos

Son programas que al momento de ejecutarse dentro del computador se realizan copias de este y una de las principales características es la propagación mediante la red de una empresa dejando a su paso computadores colapsados impidiendo trabajar a los usuarios. Los gusanos a diferencia de los virus no atacan archivos sino específicamente el rendimiento de sus ordenadores. (Rivero, 2018)

Los gusanos utilizan los correos electrónicos para propagarse por la red un ejemplo es el envío de un adjunto como imagen o archivo de música los mismos que contienen el ejecutable del gusano al momento de abrirlo la computadora pasa a estar infectada y no tarda en expandirse por la red empresarial, interceptar a un gusano es una tarea sumamente complicada ya que al momento que un computador lo localiza se traslada a otra computadora para seguir infectado la red. (F-Secure, 2018)

Los gusanos no roban ningún tipo de información, pero si se limita el desempeño de los ordenadores infectados y evitan que los usuarios puedan realizar sus tareas cotidianas de una manera normal, es por esto que es un ataque el cual causa muchos daños materiales en los ordenadores y es muy difícil de eliminar completamente de una red empresarial.

1.2.4.1.4. Troyanos

Un troyano es catalogado como un virus, aunque no cumple con todas las características de uno de ellos, pero por su forma de propagación y de actuar dentro del sistema fue catalogado como un virus.

Un troyano es un programa pequeño el mismo que se encuentra incrustado o alojado dentro de una aplicación normal. Al instalar la aplicación real este pequeño programa también se ejecuta sin que el usuario tenga idea que está ejecutándose en segundo plano, ya que el atacante tiene acceso a la computadora huésped puede obtener cualquier tipo de información del usuario. (RIVERO, 2016)

Uno de los troyanos más famosos en el mundo es Zeus como su nombre lo indica es el más grande de los troyanos que existe, este troyano atacaba cuentas bancarias hasta que en el 2011 sus creadores liberaron su código desde ese momento existen nuevos troyanos con la misma finalidad utilizando código de Zeus, este troyano infectó más de 10 millones de computadores y robado cientos de millones de dólares. (Donohue, 2013).

1.2.4.1.5. Spyware

Un spyware es un programa espía que se mantiene en escucha para poder obtener todo tipo de información sobre una persona u organización sin que el usuario tenga conocimiento de que este programa se encuentra ejecutándose en segundo plano, estos programas espías tienen como objetivo ingresar en empresas publicitarias u organización especifica en busca de información con alto interés, este programa envía información periódica a un servidor en donde se aloja esta información para posterior el atacante pueda filtrar esta información y verificar que nivel de impacto tiene para la empresa. (RIVERO, 2016)

Uno de los *spyware* más famoso es *CoolWebSearch* este *spyware* es evidente ante el usuario y se puede saber que está infectado, uno de los síntomas es la página web de inicio del navegador cambiada y es complicado regresar a la configuración inicial. En la navegación normal del usuario salen aleatoriamente anuncios de diferentes

productos y en algunos casos anuncios realmente vergonzosos, pero uno de los problemas realmente graves es la navegación por páginas web que el usuario no ha pedido es en esta navegación que el usuario entrega datos importantes y hasta puede ser víctima de robo de identidad y dinero. (Stories, 2014).

1.2.4.1.6. AdWare

Este programa malicioso no genera un daño al ordenador pero genera una saturación de publicidad de productos y servicios de diferentes empresas, el objetivo es poder obtener clientes mediante la publicidad en ventanas emergentes, o a través de herramientas que se incrustan dentro del navegador y al mantenerse ejecutando genera un número grande de publicidad mientras se navega por la web. (RIVERO, 2016)

Uno de los *adWare* más conocidos es *DNS Unlocker* es realmente agresivo ya que se oculta detrás de una aplicación para quitar publicidad en realidad quita publicidad de algunas páginas, pero muestra anuncios de otras páginas y al momento de hacer *click* sobre ellas se instalan nuevos *adWare* que pueden llegar a robar información personal del usuario. (Morelli, 2016).

1.2.4.1.7. Ransomware

Este código malicioso ingresa dentro de un ordenador en donde se encuentra información importante y vital para una organización y lo cifra, el atacante da una serie de instrucciones para que el usuario pueda recuperar su activo más importante la información. Para que el atacante pueda dar la contraseña para poder desencriptar el ordenador pide un rescate económico, de esta manera obtiene un redito económico por este tipo de ataque. (RIVERO, 2016)

Cerber un ejemplo de ransomware que aprovecha las vulnerabilidades de las plataformas cloud, uno de sus ataques más famosos se genera a los usuarios de Office

365 y se expande por medio del correo electrónico oculta dentro de correo spam. Este ransomware tiene una nota de rescate leída por una voz generada por el ordenador secuestrado, su código se lo puede encontrar en el mercado negro. (Joseph C. Chen, 2016).

1.2.4.1.8. Phishing

El phishing es uno de los métodos más utilizados por los atacantes para poder obtener información por medio del correo electrónico utilizando ingeniería social, haciéndose pasar por empresas con renombre o personas de confianza, los atacantes utilizan todo tipo de maneras para que los usuarios caigan en su ataque, empezando con él envió de correos electrónicos hasta tener una llamada para poder obtener información personal de la víctima. (Rivero, 2018)

Un ejemplo de ataque mediante fishing es el envío de correos electrónicos con el nombre del banco como Banco BBVA o Banco Pichincha, junto a este correo con un contenido que advierte de un retiro bancario o un debito a la cuenta, hacen que el usuario se dirija a una página falsa en la cual tiene que ingresar información personal para poder anular la transacción que se menciona en el correo, este formulario que se llena es falso y la información enviada llega al atacante. (Internauta, 2014)

La información que quiere obtener el atacante puede ir desde:

- **Datos personales:** como direcciones de correo electrónico, número de documento personal, datos de localización y contacto
- **Información financiera:** como números de tarjetas de crédito, números de cuenta, información bancaria o de e-eCommerce
- **Credenciales de acceso:** como usuario y clave de redes sociales y correo electrónico

Los principales medios de propagación de fishing es el correo electrónico, redes sociales, mensajes de texto, llamadas telefónicas y la infección de malware. (Internauta, 2014).

1.2.4.1.9. *Spoofs* (Engaños)

Los atacantes siempre están dispuestos a encontrar nuevas maneras de atacar una de las entradas a los sistemas que es el correo electrónico, ya que los servidores de correo electrónico han optado por tener más seguridades contra el spam, los atacantes tenían que encontrar otra forma de poder llegar el mensaje a los usuarios, de esta manera se crea el Spoofing utilizando cuentas de correo electrónico diferente y suplantando la identidad de personas o empresas con renombre para que los usuarios pueden creer que los correos enviados son legítimos. Este tipo de ataque en el mayor número de casos de ataque va acompañado de un ataque de phishing. (Acens, 2015).

Uno de los ejemplos más comunes con Spoofing es el ataque de hombre en medio el mismo que un atacante con una computadora logra interceptar una comunicación entre dos host, lo que provoca que el atacante tenga el control en la comunicación pudiendo modificar los datos o información que lleva, este ataque puede darse con la suplantación de identidad del remitente o con la obtención de información sin que las dos personas tengan conocimiento. Si el atacante logra engañar al remitente puede extraer información sin ningún problema. (ciyi, 2010).

El objetivo de este ataque es el engaño al usuario para que sea víctima de otros tipos de ataque como el phishing o spam, es por esto que es muy difícil poder disuadir este tipo de ataque ya que los servidores de correo no logran filtrar los mails ya que los mensajes tienen un remitente valido y es ahí donde pueden los atacantes obtener

información personal, bancaria e información como usuario y contraseña de plataformas que comprometen información importante.

1.2.4.1.10. *Port Scanning* (Escaneo de puertos)

El escaneo de puertos funciona con un programa el cual permite la determinación de las características de una red o sistema de manera que puede saber qué equipos están activos los servicios que se encuentran consumiendo los sistemas operativos que utilizan y de qué forma estos están organizados.

El escaneo de puerto se los puede utilizar de una manera preventiva y una manera maliciosa. Vanilla realiza un escaneo de los 65536 puertos uno por uno verificando si están *up* o *down* dentro de un computador para poder verificar si existe una vulnerabilidad o una puerta trasera a un sistema. (CYBERPEDIA, 2017)

1.2.4.2. Ataques a correo electrónico

El correo electrónico es una de las entradas más comunes que utilizan los atacantes para poder ingresar a un sistema o red de una empresa, para esto existen algunos ataques a este servicio con diferentes fines, por medio del correo electrónico se puede obtener desde un resultado publicitario hasta poder robar una cuenta bancaria. Es por ello por lo que se va a analizar algunos ataques a correos electrónicos, un ejemplo de cómo funcionan, cual es la información que desean obtener y con qué fin necesitan esta información.

En septiembre de 2015 ESET confirmo que circulaba por internet un correo electrónico con contenido fraudulento del banco Santander, este correo buscaba obtener información bancaria y personal de su víctima.

En primer lugar el contenido del correo enviado no se encuentra dirigido específicamente con el nombre del usuario sino con el correo electrónico, existen

logotipos del banco e información relacionada con la institución, este correo electrónico fue enviado a un sin número de personas de México, entre esta personas existían usuarios del banco y personas que no tenían una cuenta bancaria en el banco Santander, este ataque fue realizado para los usuarios nuevos o que han actualizado su información recientemente y sobre todo para usuarios que utilicen los servicios de banca por internet, es por esto que el contenido del correo inserta un botón para dirigirse a la página principal de la banca.

Correo electrónico con phishing

Figura 2 Contenido de correo enviado
Fuente: (Mendoza, welivesecurity, 2015)

Al dar click en el botón Ingresar se dirige a un sitio web sumamente parecido al sitio original; sin embargo, existen algunas diferencias en especial y una de las más notorias es el URL que no tiene el nombre de la entidad bancaria.

Página web falsa banco Santander

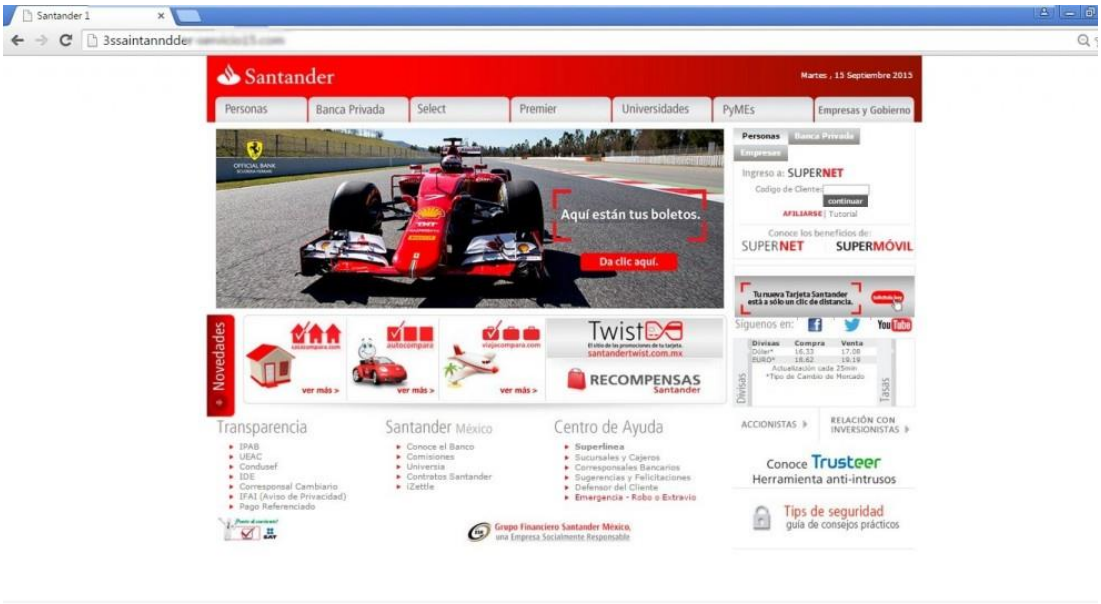

Figura 3 Página bancaria falsa
Fuente: (Mendoza, welivesecurity, 2015)

El usuario al momento de querer ingresar a la banca electrónica se solicita el usuario y contraseña y como un engaño más sugiere tener precaución con el ingreso a la plataforma esto se presenta como una advertencia para que el usuario crea que se encuentra en el lugar indicado.

Login falso página web

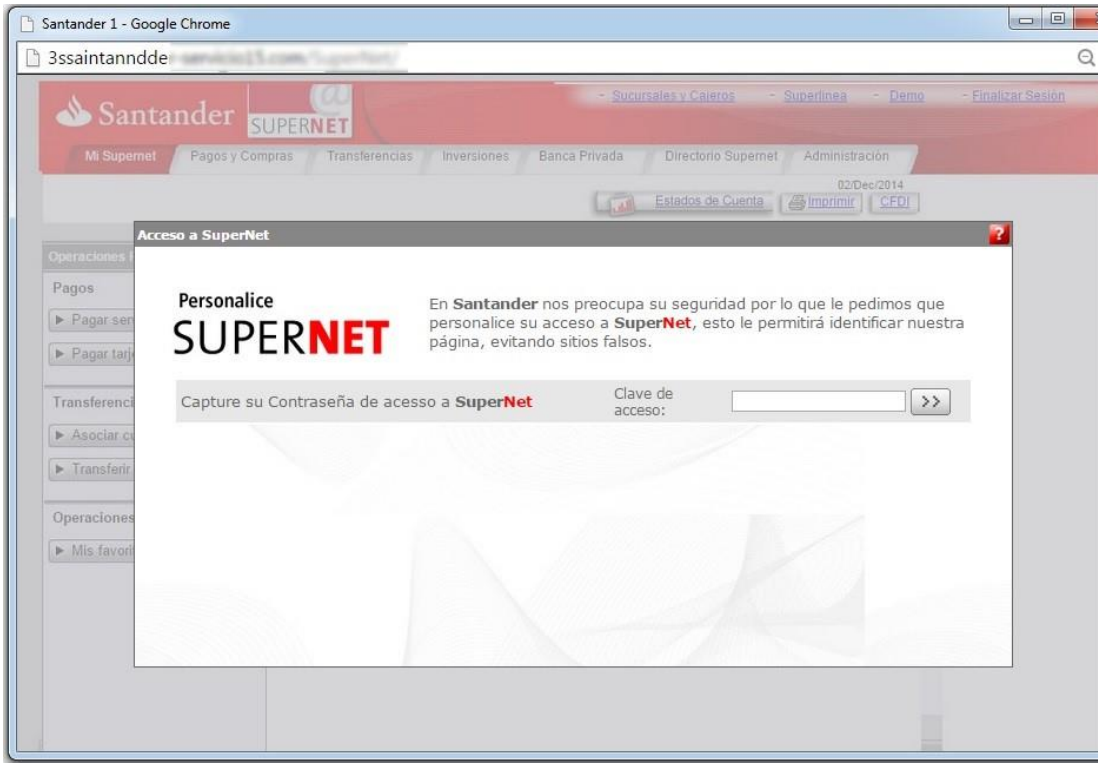

Figura 4 Ingreso usuario y contraseña
Fuente: (Mendoza, welivesecurity, 2015)

Al momento de loguearse dentro de la banca electrónica sale claramente el ataque de phishing en el momento que la pagina pide información bancaria, las entidades bancarias advierten e informan a sus usuarios que NUNCA piden información personal o bancaria por medio de correo electrónico.

Formulario falso página web

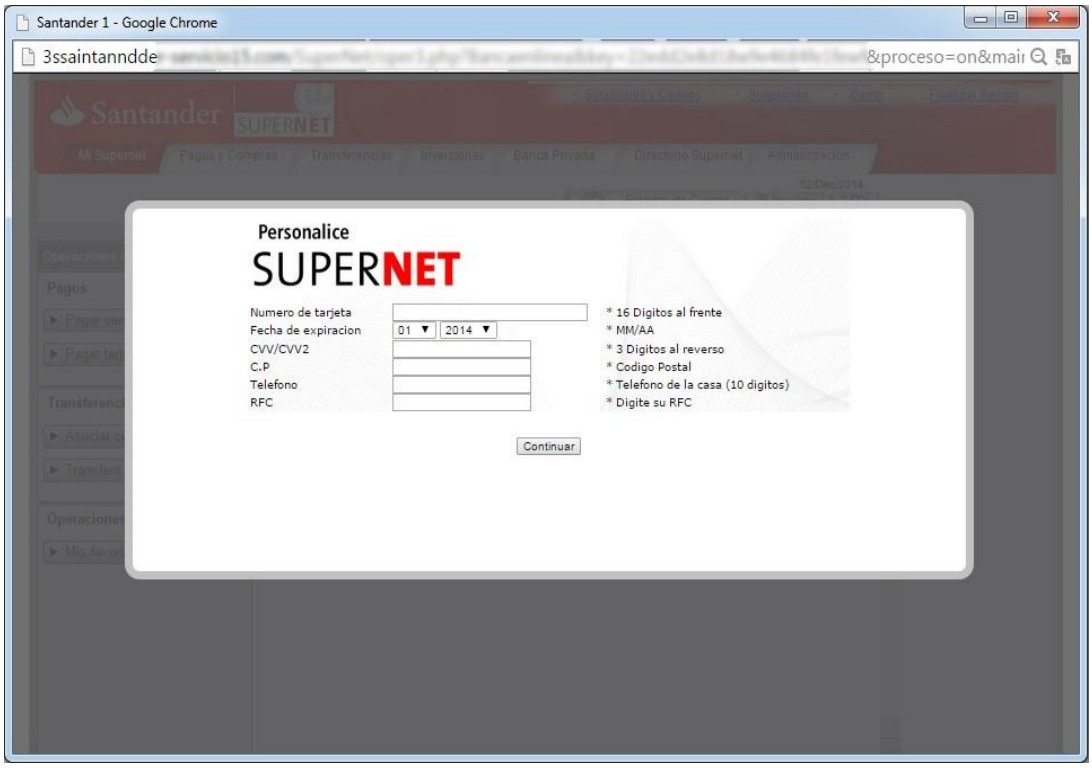

Figura 5 Ataque de phishing
Fuente: (Mendoza, welivesecurity, 2015)

Cuando el usuario es víctima de este tipo de ataques la información enviada por este medio llega al atacante y viaja por el internet sin ningún tipo de seguridad ni cifrado, poniendo aun en más riesgo los datos ingresados en la página falsa.

Datos capturados sin encriptación

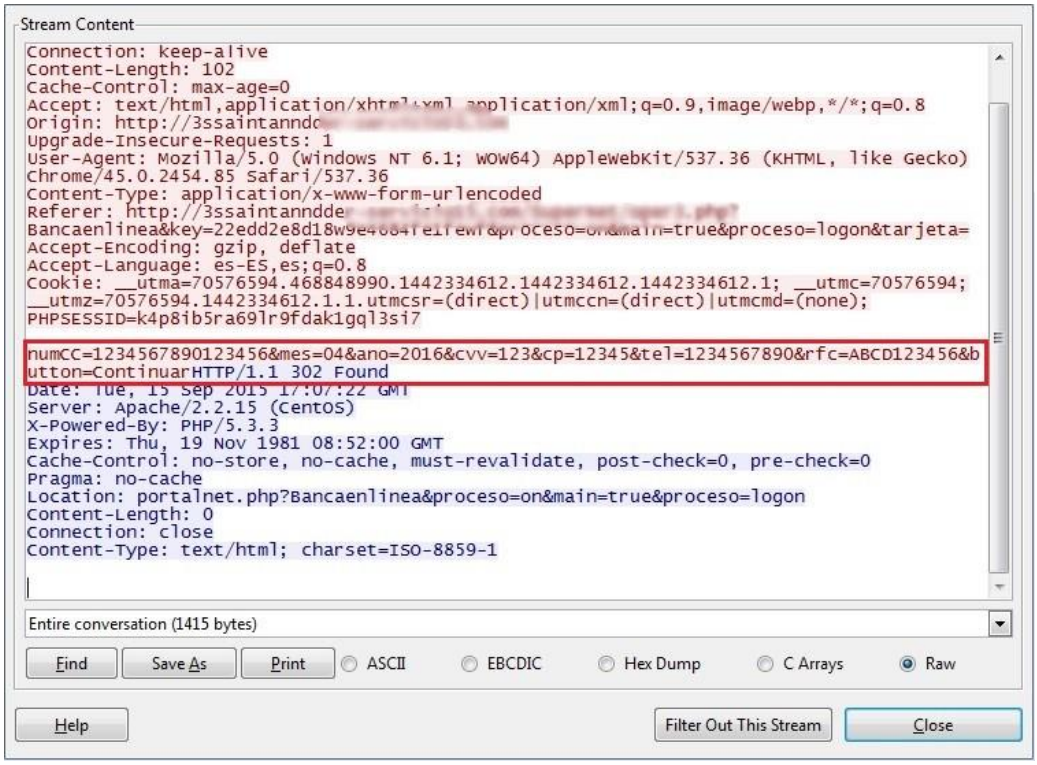

Figura 6 Datos enviados por Internet
Fuente: (Mendoza, welivesecurity, 2015)

Es así como los usuarios llegan a perder grandes cantidades de dinero y el atacante saca rédito económico por este tipo de ataques. (Mendoza, 2015)

Uno de los ataques que sacudió al mundo fue el ataque masivo al servidor de correo *Yahoo!* Por medio de dos agentes de inteligencia rusa junto a dos *crackers*, estas personas fueron responsables de tres grandes ataques al famoso servicio de correo electrónico teniendo así entre sus ataques en 2014 el robo de 1000 millones de cuentas en 2013 el robo de 500 millones y por último el robo de 32 millones de cuentas. La información que buscaban con el robo de este número gigante de cuentas de correo electrónicos fue buscar cuentas de periodistas rusos y miembros de la oposición del

presidente de Rusia Vladimir Putin, también buscando cuentas de miembros del gobierno de Estados Unidos que desempeñan labores de ciberseguridad y trabajadores de la Casa Blanca. La identidad de los dos rusos implicados son Dmitry Dokuchaev e Igor Sushchin, miembros de FSB el heredero de lo que antes se conocía como KGB.

El agente del FBI Malcolm Palmore apunta a que este tipo de ataque es un *Spea*r *phishing*, este *Spear fishing* está orientado a una entidad pública o privada en la cual se quiere obtener los datos de un integrante para así acceder a la infraestructura de la empresa o entidad.

Alexsey Belan en su análisis de componentes importantes para la organización descubrió dos: Base de datos de usuarios (UDB) y una herramienta administrativa llamada *Account Management Tools*, con estas dos herramientas prácticamente tenían la información importante ya que en la base de datos podían encontrar las cuentas deseadas mientras que con la segunda herramienta podían alterar datos de la cuenta incluido su contraseña. Al momento que tenían esta información Belan descubrió una herramienta que le permitiría falsificar *cookies* para conseguir acceso a las cuentas sin cambiar sus contraseñas. El uso de estas herramientas se realizó en dos fases: la primera fase fue desde la red interna de *Yahoo!*. Belan pudo copiar parte de la UDB a su ordenador personal mediante una transferencia de archivos FTP. La segunda fase se pudo generar *cookies* de forma externa sin entrar a la red de *Yahoo!*. El momento que llegaron a descubrir este ataque es cuando Dmitry Dokuchaev enviaba un correo a Igor Sushchin una captura de pantalla en el que aparecía un complemento de Firefox llamado *Advanced Cookie Manager*. En este ataque se conoce que fueron afectadas 6500 cuentas, no se ha revelado si el detective del FBI Malcom Palmore fue quien descubrió el ataque o el servidor de correo *Yahoo!* Ni cuanto tiempo duró la intrusión antes de ser detectada y cortada. (AGUDO, 2017)

Los ataques a correos electrónicos pueden llegar desde un SMS de texto al celular de la víctima, en septiembre del 2015 investigadores de la Universidad de Toronto junto a Panda Security emitieron un comunicado de cómo se maneja este tipo de ataque a correo electrónico mediante mensajes de texto, el primer paso que realizaban los ciber delincuentes es enviar un mensaje de texto al celular de la víctima, este mensaje contiene una alerta de información al usuario que su cuenta de correo electrónico ha sido vulnerada, después de un corto tiempo llega un correo falso de Google que advierte que se ha iniciado sesión con su cuenta de correo electrónico, junto a este mensaje de correo se adjunta un enlace que teóricamente envía al usuario a una página web donde puede cambiar su contraseña y puede cerrar todas las cuentas antes abiertas. Esta página web falsa de Google es un ataque de *phishing* en la cual el atacante puede obtener la contraseña de la víctima, la página web falsa pide al usuario el código de verificación para ingresar a su cuenta en esta caso el código que le llega al usuario es el que envía Google como seguridad, teniendo esta información el atacante está dentro del servidor de correo electrónico. En tan solo 2 pasos los atacantes pudieron vulnerar un servidor de correo electrónico público como lo es Gmail. (Tecnología, 2015).

Kasper sky Lab informo que ha detectado un número gigante de correos electrónicos dirigidos a los usuarios de 400 organizaciones industriales la mayor parte de estas en Rusia, estos correos contenían información de compras y contabilidad, se descubrió un ataque de *Spear Phishing*. Kaspersky informa los pasos que realizaron los atacantes para poder obtener el acceso a los correos electrónicos, el primer paso fue crear una carta dirigida específicamente a la persona escribiendo su nombre, es decir los atacantes crearon una carta para cada usuario, el contenido del correo adjuntaba un archivo malicioso, el usuario al dar click en el adjunto se activa la instalación de un programa legítimo modificado sin que el usuario se diera cuenta. Este programa logró

que el atacante se pueda conectar, examinar documentos y otros programas de finanzas y contabilidad. Los ciber delincuentes instalaron programas de espías y herramientas de administración remota para poder conectarse al ordenador. (Portaltic, 2018).

El ataque realizado a Epsilon que es uno de los más grandes proveedores de servicios de marketing teniendo entre sus principales clientes a: Disney, Citbank, JP Morgan Chase, Marriott Rewards, Ritz Carlton. Epsilon asegura que este ataque, solo él, afectó al 2% de sus clientes a los que presta servicios de correo electrónico.

Este ataque tenía como objetivo cuentas de usuarios específicos a los cuales enviar correos maliciosos los cuales tienen un alto porcentaje de ser engañados, claramente es un ataque de *Spear-phishing* en la cual con la información robada pueden enviar correos con contenido de las marcas y clientes que da servicio esta empresa. (TI, 2011)

En mayo del 2017 se realizó el ataque más sofisticado a Google Docs. Por medio de correo electrónico, este correo era enviado con el contacto de una persona conocida en el cual menciona que se ha compartido un documento y se presenta un botón que indica Open in Docs.

Ataque Google Docs

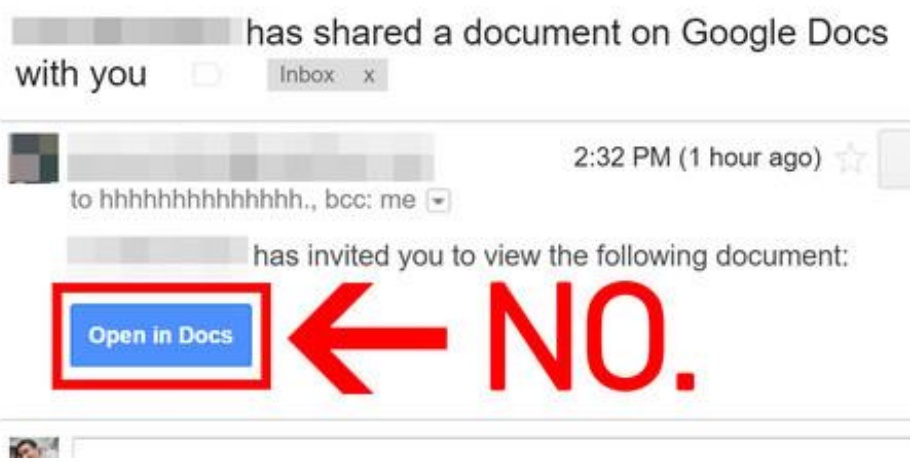

Figura 7 Ataque de Phishing Google Docs
Fuente: (ÁLVAREZ, 2017)

Lo que género que a este correo no lo detectaran como un ataque de p*hishing* fue que era enviado por un contacto conocido y era completamente creíble para los usuarios. Los pasos que siguieron para este ataque fueron: primero se recibe un correo electrónico de un conocido que invita a revisar un documento de Google Docs, segundo dando click en el botón inicia una página en la cual se pregunta con qué cuenta de correo electrónico de Gmail va acceder, posteriormente se ejecuta una página en la cual pide otorgar permisos que para el usuario se otorgaba a la aplicación de Google Docs, al presionar el botón de Permitir esta aplicación tiene acceso al correo electrónico con los privilegios de enviar y leer así como a la información importante que ellos desean la lista de contactos del usuario.

Permisos falsos Google Docs

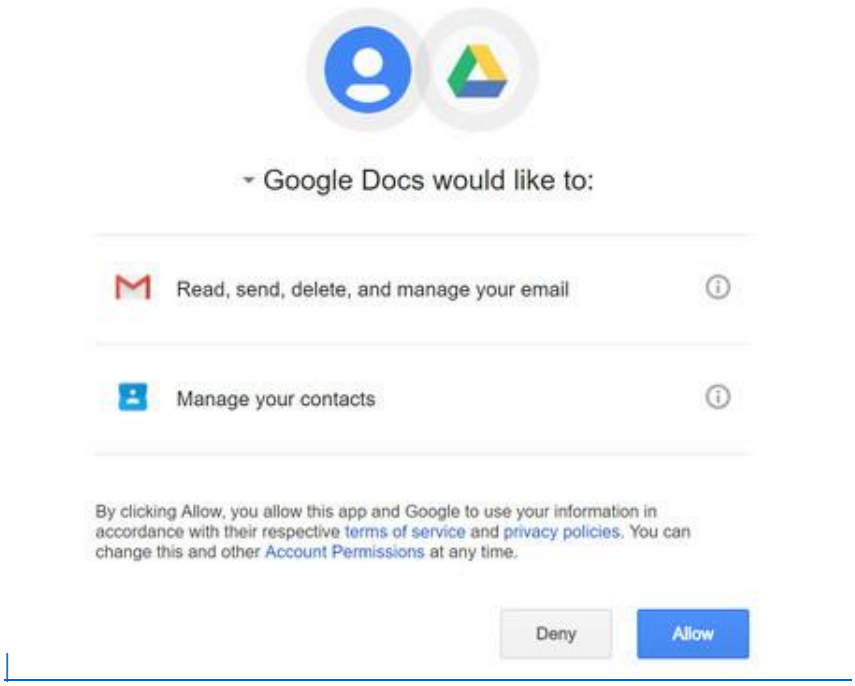

Figura 8 Permisos falsos Google Docs
Fuente: (ÁLVAREZ, 2017)

El atacante inmediatamente envía correos a todos los contactos del usuario haciendo así que el ataque de *phishing* se propague de forma imparable. (ÁLVAREZ, 2017)

Un ataque de *phishing* utiliza en todos los casos un ciclo que corresponde al siguiente.

Ciclo de pishing

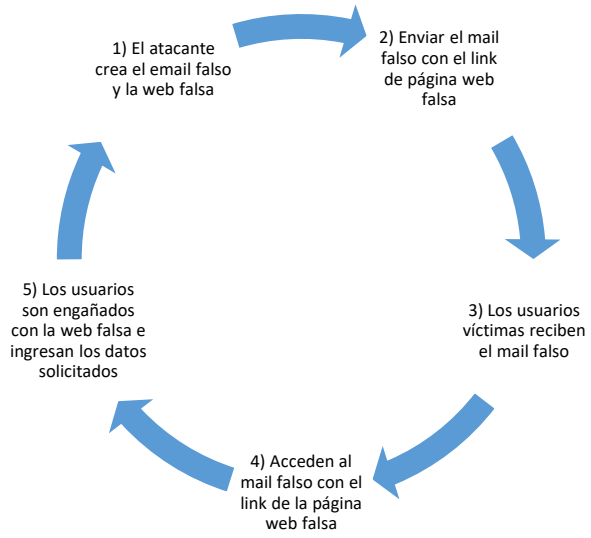

Figura 9 Ciclo de un ataque de Phishing
Elaborado: Francisco Alvear

En los casos investigados por las autoridades por Phishing, estadísticamente en el año 2008 existen más casos resueltos que denunciados, esto se debe a que la información que tenían las personas sobre este tipo de ataques no era de conocimiento de todos, pero las autoridades pudieron resolver más ataques que los denunciados. En los siguientes años el panorama ha cambiado existe un número mayor de casos denunciados que resueltos, esto da como conclusión que los ataques continúan, pero de una manera más efectiva y los atacantes dejan menos pistas para que los casos sean resueltos.

Mientras existen nuevas maneras de seguridad los atacantes siempre se mantienen en constante aprendizaje para poder vulnerar estas nuevas tecnologías.

Casos de phishing

Figura 10 Casos investigados de phishing
Fuente: (ÁLVAREZ, 2017)
T

1.3. Solución para mitigar ataques cibernéticos

Los atacantes siempre buscan las vulnerabilidades de un sistema, para esto los especialistas en seguridad informática tratan de que esas vulnerabilidades no existan y el sistema esté seguro. A continuación, tenemos soluciones a ataques a correos electrónicos que se obtienen luego de obtener los resultados de la presente investigación:

1.3.1. Solución a *Spoofing*

Una de las preocupaciones de los usuarios es que suplanten su correo electrónico y se puedan enviar mensajes los cuales atenten contra su integridad o prestigio, es por esto que las cuentas de correo electrónico son los principales objetivos de los atacantes, para esto se deben tomar en cuenta las siguientes recomendaciones:

- Cuando se ha suplantado la identidad de un email es importante revisar si fueron enviados desde el mismo servidor de correo electrónico o fueron enviados por medio de programas de suplantación de identidad
- Comprobar el estado de la cuenta con el proveedor de hosting o servicio de correo electrónico.
- Si los correos electrónicos se envían del ordenador se debe proceder a la búsqueda de un virus o programa que esté realizando esta función.

El método más eficaz para poder eliminar el *Mail Spoofing*, es mediante la utilización de registros SPF (*Sender Policy Framwork*) esta función utiliza registros del dominio desde el cual se está enviando el correo electrónico, de esta manera si se intenta suplantar la identidad con un programa o se envía un correo desde otro dominio, el correo electrónico será considerado como no auténtico y se enviará a la bandeja de spam o bien el servidor de correo no permitirá que sea entregado. (Acens, 2015)

1.3.2. Soluciones a ataques tipo *Phishing*

El ataque por *phishing* se ha vuelto muy común entre los usuarios de correo electrónico por la búsqueda información personal del usuario. Estas son algunas consideraciones para no ser víctima de un ataque de *phishing*.

- Las entidades bancarias o empresas nunca pedirán información personal o bancaria por medio de correo electrónico.
- Si el remitente del correo electrónico o contenido es desconocido, jamás se puede dar click en ningún enlace que contenga el correo.
- Si el usuario piensa que el link que contiene el correo si es verdadero se sugiere no dar click en el mismo, sino escribir este link en el navegador y verificar la fuente de la página web

- Verificar con la entidad bancaria o empresa que el correo electrónico enviado es verídico y si el contenido del correo pide información para qué se va a utilizar esa información
- Al ingresar a una página web, verificar si la página contiene un https:// seguro junto a su candado de seguridad SSL.
- Verificar el nombre de la empresa o servicio en el url del navegador, los enlaces falsos suelen contener letras adicionales a la url verdadera. (Rivero, 2018)

1.3.3. Técnicas de mitigación aplicadas al *Spear Phishing*

- **Control de aplicaciones:** Dos de las aplicaciones más riesgosas son las páginas web y el correo electrónico a menudo es por donde los atacantes siempre empiezan su ataque, el *malware* es uno de los virus más comunes, se puede tomar varias medidas de seguridad sobre las aplicaciones, pero eso haría que perdieran la funcionalidad de estas para ello una de las soluciones es ejecutar las aplicaciones peligrosas en máquinas virtuales separadas. Si en algún momento el ataque se lleva a cabo primero la máquina virtual no tiene información relevante que le sirva a los *hackers*, segundo si atacan la máquina virtual y la corrompen no dañan el computador físico o local, este mecanismo de seguridad hace que cuando la aplicación está cerrada (La máquina virtual está apagada), cualquier ataque perjudicial también está controlado. En este caso una máquina que está infectada estará así en un periodo corto y controlado, y existe un ambiente controlado en la física de equipos mientras que en la parte de red es un tema completamente diferente ya que el ataque puede expandirse a la red empresarial.
- **Filtrar el contenido perjudicial:** En mucho de los casos de ataques exitosos la actividad que se utiliza para poder comprometer un sistema o red vienen en

un entorno de archivos adjuntos en un correo electrónico, macros en documentos de office y en contenidos de HTML de páginas web, en las organizaciones se utiliza frecuentemente el correo electrónico para poder enviar archivos adjuntos pero no es necesario que todos los usuarios de la organización tengan este privilegio para lo cual si no es necesario se debe bloquear completamente. Bloquear estratégicamente ciertas actividades dentro del correo electrónico a usuarios que no necesiten este privilegio tiene un impacto importante en la minimización de los daños que causan estos ataques dentro de la empresa.

- **Limitar el contenido ejecutable:** El bloquear un archivo ejecutable en la mayoría de los casos es efectivo excepto si los archivos son necesarios para el usuario para lo cual las empresas tratan de utilizar dos cuentas de usuarios tanto la de administración o sistemas como la cuenta personal del usuario. Para que el usuario pueda ejecutar una aplicación se debe poner la clave de administrador en este caso es un filtro efectivo para saber qué clase de programas el usuario puede o no tener dentro de su computador.
- Otra de las opciones es utilizar programas que pueden escanear los archivos ejecutables para determinar si son seguros si son maliciosos automáticamente los bloquea o borra del sistema operativo, con la utilización de estas herramientas ofrece a la empresa una mayor flexibilidad en la ejecución de aplicaciones, pero también se limita que aplicaciones con otros fines entren al sistema y puedan obtener información de éste.
- **Control de ejecutables:** Uno de los principales problemas de una empresa es creer que la mayoría de los ataques vienen de fuera de la empresa, pero existen también riesgos dentro de la empresa. Como ejemplo un "*insider*" que es una

persona que tiene un conocimiento amplio de la empresa, su modelo de negocio y sobre todo tiene acceso a información relevante y por situaciones adversas dentro de la empresa busca una manera de dañar o vengarse de su situación actual. El *insider* por tener acceso a información puede realizar acciones como el cambio de claves dentro de aplicaciones o servidores y el uso inadecuado de dispositivos en la empresa.

1.3.4. Soluciones a *Spamming*

El correo SPAM o correo basura es muy molesto para el usuario que tiene el servicio de correo electrónico, adicional puede llegar afectar el funcionamiento óptimo del servidor de correo llenando la bandeja de entrada y evitando que los correos se envíen, es por esto por lo que se tienen las siguientes soluciones para evitar el *Spamming*.

- No responder correos electrónicos con contenido que no se ha solicitado, ya que al contestar este correo verifica que la cuenta a la que fue enviada está activa y llegan muchos más mails a esta cuenta.
- No proporcionar datos por medio de correo electrónico o por medio de link que estén contenidos dentro de estos mails no fiables
- No llenar ningún tipo de formularios online, ya que la información que se ingresa sirve para ser vendida o sirve para un inicio de spam ya que uno de los datos importantes que se pide dentro de este formulario es el correo electrónico.
- No ingresar el correo empresarial para registro de cuentas en sitios o publicidad, es recomendable utilizar una cuenta personal específica para este tipo de registro a páginas o anuncios.
- Crear correos electrónicos no habituales y que el programa de producción aleatoria no pueda descifrar y ser víctima de SPAM. (ValorTop, 2017).

1.3.5. Soluciones a Gusanos

Los gusanos informáticos es uno de los ataques más silenciosos que existe, el personal de seguridad informática llega a tener conocimiento de que su red está infectada con gusanos cuando en su rastro deja un sin número de ordenadores dañados o con problemas técnicos, la propagación de gusanos puede ser muy rápida como se puede tomar su tiempo, pero uno de los verdaderos problemas de un ataque con gusanos es poder eliminarlo por completo de la red. Es por esto que se generan diferentes tipos de soluciones para poder evitar que los gusanos puedan ser ejecutados en un ordenador y se expanda a los computadores de la organización.

- Los gusanos llegan por medio de archivos adjuntos a correos electrónicos, es por esto que se recomienda verificar la fuente del correo electrónico y no dar click sobre el archivo por que podría ejecutar el gusano en el ordenador.
- Tener un antivirus actualizado es una ventaja para el usuario ya que protegerá el ordenador y verifica los archivos que se van a ejecutar dentro del ordenador.
- Mantener cada cierto tiempo un análisis completo del ordenador con el antivirus.
- Los ordenadores MAC son más propensos a distribuir el gusano por la red sin que el usuario final tenga conocimiento, es por esto por lo que se recomienda tener todas las actualizaciones del sistema operativo
- Los dispositivos que tienen un sistema operativo Android han logrado mantener a los gusanos fuera de su sistema, pero pueden ser vulnerables a otro tipo de ataque como el *adware*. (wikiHow, 2016).

1.3.6. Solución a Fuerza Bruta o Bomba de Correos

Los ataque de fuerza bruta a correos electrónicos se dan ya que los usuarios finales no utilizan las políticas de seguridad para la generación de claves para el servicio, cuando

se trata del sistema operativo Windows, el método de autenticación y configuración de privacidad de bloque es una de las maneras que evitan los ataques de fuerza bruta por que hacen que estos sean mucho más lentos.

Es importante no utilizar conexiones directas a la base de datos con usuario y contraseña ya que pueden ser interceptadas y generar que el ataque de fuerza bruta se convierta en un ataque de denegación de servicio y el servicio de base de datos llegue a caer, una de las soluciones que se han implementado en las cuentas de correo electrónico son la autenticación de dos pasos, el mismo que consiste que si el atacante llega a obtener el correo y logra descifrar cual es la contraseña del usuario, el siguiente paso para ingresar al sistema es el envío de un mensaje de texto o llamada telefónica con un código con el cual el usuario original podrá ingresar al sistema, el atacante no tendrá esta información ya que el mensaje de texto se envía al número telefónico personal. (Ramiro, 2018).

- Este sistema de protección se implementa para asegurarse que los adversarios tienen que evitar o vencer numerosos componentes del sistema de manera secuencial. Esto crea pasos adicionales que el adversario debe tomar para vencer al sistema, requiere una gran planificación para vencer al sistema, y reduce la probabilidad de vencimiento del mismo. La defensa en profundidad también retrasa al hacker, proporcionando por tanto oportunidades adicionales de detectar y responder a un suceso.
- Consecuencias mínimas del fallo de un componente: Introduce la planificación de contingencias en los sistemas de protección, para mitigar las vulnerabilidades de los sistemas ante los fallos de componentes o el fracaso del sistema de protección.

- Protección equilibrada: Las aplicaciones y componentes individuales del sistema de protección se integrarán y convergerán de tal manera que proporcionen un mismo nivel de protección. Cada aplicación o componente del sistema de protección puede ser diferente física o estructuralmente, pero trata y mantiene un nivel adecuado de protección frente a los riesgos al equilibrar la integridad, la seguridad y los costos estructurales.

1.4. Correo Electrónico

Cuando se habla de correo electrónico llegan a la mente servidores muy comunes como *Gmail, Outlook* o el antiguo *Yahoo!!*, se tiene una variedad de correos electrónicos los cuales están montados en diferentes sistemas operativos tanto en *Windows* como *Linux* de la misma manera existen muchos tipos de motores con diferentes interfaces, algunas más amigables para el usuario, pero se tiene una opción adicional que es montar un propio servidor de correo electrónico, ¿Para qué tener un correo electrónico si existen correos que se administran de forma gratuita?, para ello se debe analizar tanto ventajas como desventajas de tener un propio correo electrónico.

En el estudio de la seguridad del correo electrónico, tener un propio servidor de correo tiene una gran desventaja que es la seguridad es por eso por lo que el control de los usuarios, contraseñas seguras, autenticación, actualización y disponibilidad del servidor recae sobre el administrador del correo electrónico.

El correo electrónico tiene muchas características importantes que hacen que sea uno de los medios de comunicación más usados en este tiempo ya que es un medio eficaz y económico para la comunicación entre personas.

La rapidez es una de las cualidades importantes del correo electrónico ya que prácticamente el tiempo que lleva el envío de un correo electrónico desde su emisor a su receptor es inmediato dependiendo de dónde estén localizados los usuarios.

Tomando en cuenta la velocidad y que el costo de la comunicación es prácticamente una llamada local o de teléfono celular, se tiene como conclusión que a comparación de los medios de comunicación ya conocidos como correo postal, teléfono e inclusive fax, el correo electrónico es el más económico de todos.

La velocidad de envío y recepción de mensaje ha hecho que los usuarios finales cambien los hábitos de escritura haciendo que el contenido de los correos sea menos formales y más concretos.

El internet funciona las 24 horas del día los 365 días del año, por lo cual el correo electrónico siempre está activo excepto en raros casos de caída del servidor, problemas principales de red o problemas con el ISP los mensajes de correo electrónico se quedan en espera hasta poder llegar o caso contrario regresa una alerta con un aviso del inconveniente.

En la actualidad el uso del correo electrónico en empresas o correos personales hacen que esto evite el uso de papel para la escritura de mensajes, cartas o solicitudes lo cual ayuda a la conservación de los recursos naturales.

Los correos electrónicos actualmente tienen muchas características importantes como la creación de grupos de usuarios diferentes, si se necesita enviar un correo a un grupo específico de personas se elige el grupo y se envía el contenido deseado.

1.5. La arquitectura de correo electrónico tiene 4 elementos fundamentales:

- Cliente de correo (MUA). Ofrece los mecanismos necesarios para la lectura y composición de los mensajes de correo.

- Servidor de salida (MTA). Recibe el correo electrónico y lo envía al servidor de entrada del dominio del receptor.
- Servidor de entrada (MTA). Almacena los correos electrónicos enviados a los buzones que gestiona y cuando un cliente consulta su cuenta le envía los correos electrónicos que ha recibido.
- Agente de acceso. Se encarga de conectar un agente de usuario al mensaje almacenado mediante protocolos de aplicación como POP e IMAP.

Arquitectura correo electrónico

Figura 11 Arquitectura de correo electrónico
Fuente: (Acens, 2015)

Para comunicar los sistemas que componen la arquitectura de un correo electrónico se disponen protocolos para poder comunicarse entre ellos:

- Simple *Mail Transport Protocol* (SMTP) se encarga del transporte de los mensajes de correo electrónico.
- *Postal Office Protocol* (POP) e *Internet Message Access Protocol* (IMAP) ambos protocolos se encargan de la comunicación entre los agentes de usuario (MUA) con los agentes de entrega de correo (MDA) adicional permiten la gestión por parte de los usuarios a sus buzones de correo electrónico.

El funcionamiento del servidor de correo electrónico se basa en una aplicación amigable para el usuario final donde tiene algunos mecanismos necesarios para escribir, recibir y contestar mensajes, existen varias interfaces del servidor de correo electrónico, el objetivo en sí de la interfaz es que puedan realizar las funciones: recepción, composición y ordenación mediante carpetas y subcarpetas del correo electrónico.

Como primer punto el cliente lo primero que realiza es la lectura de los correos que se encuentran en las bandejas de entrada y su presentación al usuario indicando la fecha de entrega, quien envió el correo, si se ha leído o no el correo, la prioridad del correo y un asunto que es el título del correo así se puede ver la prioridad de éste, para usar el correo electrónico se pueden usar los protocolos antes mencionados POP e IMAP. La principal diferencia entre ambos protocolos es que POP realiza la gestión del correo sobre el equipo desde el que se conecta el cliente mientras que IMAP realiza la gestión sobre el servidor, los pasos que el sistema realiza para la entrega del mensaje son:

- El cliente se conecta al servidor de salida y le proporciona el mensaje a enviar el mismo se dirige a la bandeja de borradores en estado de cola de espera definida por el servidor.
- El servidor de salida revisa su cola y encuentra el mensaje de espera en ese momento empieza el proceso de transmisión al destinatario, obteniendo la dirección del servidor de destino mediante el sistema de nombres de dominio.
- Se establece una conexión TCP entre el servidor de correo entrante del servidor de destinatario enviando una copia del mensaje que se encontraba en espera. Una vez que el servidor de salida origen y el servidor de entrada del destinatario acuerdan la recepción del mensaje, el servidor de origen borra su copia local

del mensaje en este caso la bandeja de borradores y pasa a la bandeja de mensajes enviados.

- Si en el proceso ocurre algún fallo, el proceso de transferencia del correo registra la hora en que se intentó enviarlo y es enviado a la cola de espera hasta que un nuevo proceso empiece, si transcurrido un cierto tiempo el correo no se pudo enviar se devuelve un mensaje informando el error al cliente.

Diagrama de flujo procedimiento de envío de correo electrónico

Diagrama de flujo envió correo electrónico

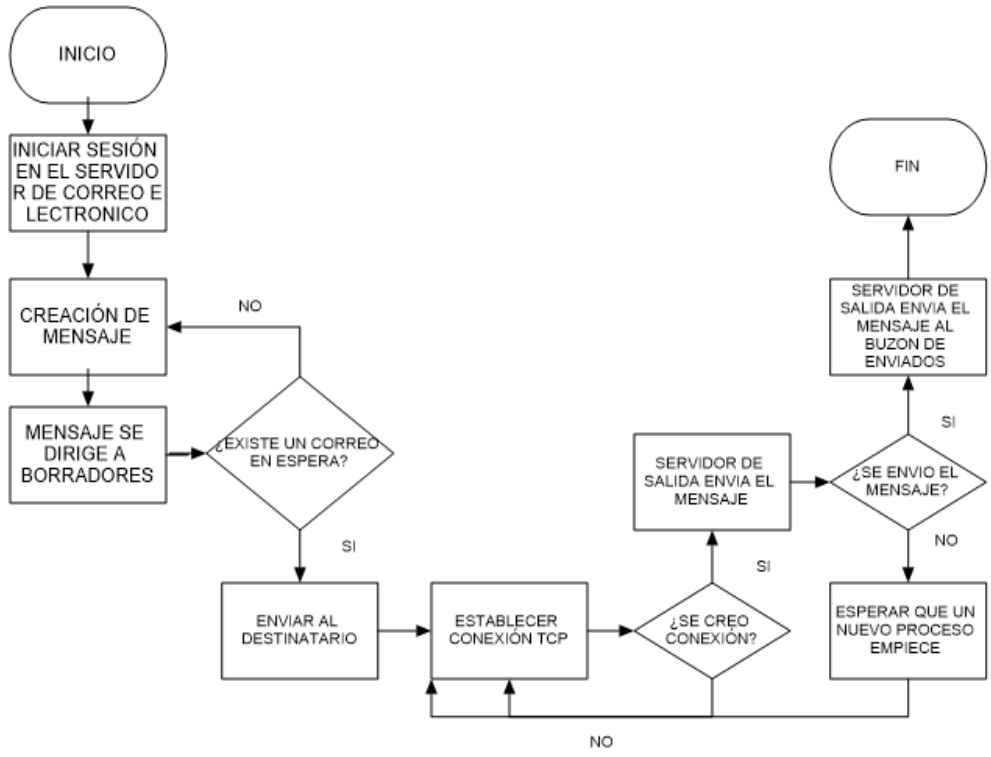

Figura 12 Diagrama de flujo procedimiento de envío de correo electrónico
Elaborado: Francisco Alvear

1.5.1. Ataques Informáticos

Con el avance tecnológico tanto de los medios tecnológicos como los medios de comunicación han generado mayor número ataques y nuevas modalidades de robo de

información que han transformado la conexión a Internet en un aspecto sumamente hostil para cualquier tipo de empresa u organización.

En años anteriores las personas con grandes conocimientos en el campo informático a quienes les apasionaba la investigación con el ánimo de tener más conocimiento en su especialidad sin hacer ningún tipo de daño a la empresa era bien visto por el ambiente informático, en la actualidad este tipo de prácticas se han convertido en un grave problema para la organización, ya que estas personas con grandes conocimientos ocupan el mismo en hacer daño a la empresa y así poder obtener, dañar, modificar o robar el activo más importante de la empresa que es la información pudiendo así obtener un rédito tanto económico o simplemente el conocimiento de la sociedad de las capacidades que puede tener esta persona.

Bajo este concepto los *hackers* realizan una investigación de las vulnerabilidades por donde pueden ingresar a la red de la empresa para así poder ver su información, uno de los medios más utilizados para realizar esta acción es el correo electrónico, pero para poder lograr mitigar de una manera eficiente los ataques provocados es muy importante saber de qué manera atacan y cuáles son los puntos débiles de los sistemas informáticos los cuales siempre son motivo de vulnerabilidad y es en los cuales se debe poner énfasis y enfocar los esfuerzos de seguridad.

1.5.1.1. Fases de un ataque informático

El pensar como un atacante en la parte de seguridad informática nos mantiene un paso delante de ellos, pero jamás se debe subestimar su mentalidad, para eso se debe conocer las fases de un ataque informático. La siguiente imagen muestra las cinco etapas por las cuales suele pasar un ataque informático al momento de ser ejecutado.

Fases de un ataque informático

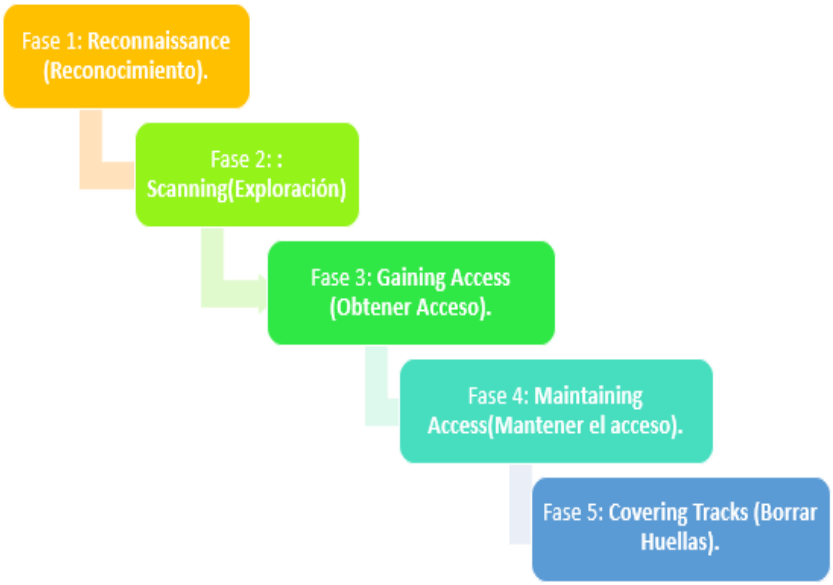

Figura 13 Fases de un ataque informático
Elaborado: Francisco Alvear

- **Fase 1: *Reconnaissance* (Reconocimiento).** Es la primera etapa en la cual el atacante busca información importante sobre la organización por lo general en esta fase la información se la obtiene de Google para saber cuál es el giro del negocio de la organización y así se obtiene datos importantes para la siguiente fase. Alguna de las técnicas utilizadas en esta fase es: El *dumpster*, el *sniffing* y la Ingeniería Social.
- **Fase 2: *Scanning* (Exploración).** En la segunda etapa se utiliza la información obtenida en la primera etapa así pueden sondear el blanco y tratar de obtener información clave sobre la organización como: nombres de host, datos de autenticación y algo muy importante en la red que son las direcciones IP. Alguna de las técnicas y herramientas que se utilizan en esta fase se tiene:

network mappers, port mappers, network scanner, port scanner y vulnerability sacanners

- **Fase 3: *Gaining Access* (Obtener Acceso).** En esta fase es donde el atacante ya empieza a realizar el ataque con la información de la fase 1 y 2 empieza a explotar las vulnerabilidades y defectos que encontró en el sistema. Algunas técnicas para poder realizar el ataque son: *Buffer Overflow, Denia lof Service (DoS) Distributed Denial of Service (DDoS), Password filtering y Session hijacking*
- **Fase 4 *Maintaining Access* (Mantener el acceso).** En esta fase el atacante ha logrado entrar al sistema con alguna de las técnicas previstas en la fase anterior y lo que hará es implantar herramientas que le permita ingresar al sistema a futuro desde cualquier parte donde tenga acceso a Internet. Alguna de las técnicas que utilizan son recurrir a utilidades*: Backdoors, rootkits* y troyanos.
- **Fase 5 *Covering Tracks* (Borrar Huellas).** En esta fase el atacante obtuvo la información que quiso y ya que obtuvo acceso al sistema, lo siguiente será eliminar cualquier rastro que ha dejado al ingresar al sistema y así los profesionales del sistema o el administrador de la red no sepan que él estuvo dentro, para ello lo que el atacante eliminará son archivos de registro LOG o de alarmas del Sistema de Detección de Intrusos IDS.

1.5.1.2. Aspectos de seguridad que compromete un ataque

En la seguridad informática existen cuatro elementos fundamentales que son el mayor objetivo que los atacantes tratan de comprometer. Los elementos son la confidencialidad, la integridad, la autenticación y la disponibilidad de recursos del sistema.

Bajo estos cuatro elementos el atacante tratará de explotar alguna de las vulnerabilidades para así poder encontrar una debilidad en alguno de estos elementos.

- **Confidencialidad:** Un atacante puede estar atentando contra la confidencialidad de una persona de la organización al robar información importante como contraseñas u otros tipos de datos que viajan a través de las redes confiables y así poder tener acceso a información que solo esa persona la puede tener. Un ejemplo en el cual se encuentra un ataque de confidencialidad es el envenenamiento de la tabla ARP (*ARP Poisoning*).
- **Integridad:** Un atacante podría interceptar un mensaje que se está transmitiendo a través de un protocolo de comunicación dentro de la red, en la cual el atacante cambia un bit del texto cifrado con el objetivo de alterar los datos del criptograma, este ataque se lo conoce comúnmente como *BIT-FLIPPING* y son considerados como ataque a la integridad de la información.
- **Disponibilidad:** Uno de los ataques que son más comunes y que se puede ver un ejemplo de ataque a la disponibilidad del servicio son *DoS* en el cual el atacante podría utilizar los recursos como el ancho de banda de la conexión del ISP para inyectar un número gigantesco de mensajes y forzar la caída de éste, negando así este servicio a los usuarios que realmente están utilizando el sistema.
- **Autenticación:** En la autenticación se debe saber que la persona con la que se están comunicando es la persona correcta, los ataques más conocidos implican engañar al sistema y se realiza tomando las sesiones ya establecidas por la víctima y así el atacante pueda obtener el usuario y contraseña de la víctima a la cual está suplantando.

1.5.1.3. Ataques a correos electrónicos

El correo electrónico es una de las brechas de seguridad más fuerte dentro de una organización ya que es un punto de entrada el cual los *hackers* utilizan como vulnerabilidad para ingresar a la red.

La mayor parte de los ataques a correos electrónicos no necesitan altos recursos al contrario utilizan recursos mínimos del sistema, sin embargo, son difíciles de combatir. Las buenas prácticas en seguridad informática sugieren tener controles de seguridad preventivos tanto en la capa física como capacitación a los usuarios finales quienes son los puntos más vulnerables.

Los ataques más conocidos son:

- Correo no deseado (*spam*)
- Ataque de suplantación de identidad (*spoofing*)
- Ataques de denegación de servicio (*DoS*)
- Ataque de *Phishing*
- Ataque de *man in the middle* (hombre en medio)

Los expertos quieren determinar cuál ataque es más fuerte, pero es imposible decidirlo ya que existen un número inimaginable de ataques y cada uno de ellos ataca desde la capa de red hasta la capa de aplicación en un sistema y algunos de los ataques llegan hasta atacar la mente de los usuarios utilizando técnicas de ingeniería social los cuales confunden y hasta engañan a una persona para poder atacar su PC.

1.5.1.4. Ejemplo de ataque real: "*Spear Phishing*"

El *Spear Phishing* fue el ataque que inicio el incidente de *hacking* de *Sony Picture Entertainment*, el cual empezó desde que un usuario dentro de la organización abrió

un correo electrónico dirigido a él con su cuenta de correo empresarial el mismo que hizo *click* en un enlace malicioso y dejo que los *hackers* ingresen a la red.

Los *hackers* se quedaron dentro de la red durante meses mapeando la infraestructura y recolectando datos importantes de la empresa preparándose para mantener los datos de la empresa como rehén. Los atacantes hicieron conocida su presencia dentro de la organización a finales de año se adjudicaron el ataque y liberaron datos humillantes públicamente a lo largo de varios meses de agonía en una serie de ocho vertederos de información humillante y denigrante para la empresa. Para poder controlar los ataques tenemos algunas maneras efectivas de hacerlo.

CAPITULO 2

ANALISIS Y DISEÑO

2. Configuración de servidor de correo *Postfix* en *Ubuntu*

2.1. Requerimientos de máquina virtual *Amazon Web Service*

Para la instalación del servidor de correo electrónico se utilizó la herramienta *Amazon Web Service* la misma que nos permite implementar servicios en máquinas virtuales, en este caso se utilizó una máquina virtual *Ubuntu Server 16.04 LTS (HVM), SSD Volume Type 64-bits*, en los requerimientos de la máquina virtual existe una opción gratuita la misma que entrega:

- vCpu: 1
- Memoria RAM: 1 GB
- Disco: 8 GB
- IP Pública: 3.16.224.187
- IP Privada: 172.31.42.67

En la creación de la máquina virtual se genera un archivo con una llave privada para la conexión por medio de PuTTY, el navegador presenta la siguiente información cuando la instancia ha sido creada exitosamente.

Instancia virtual AWS

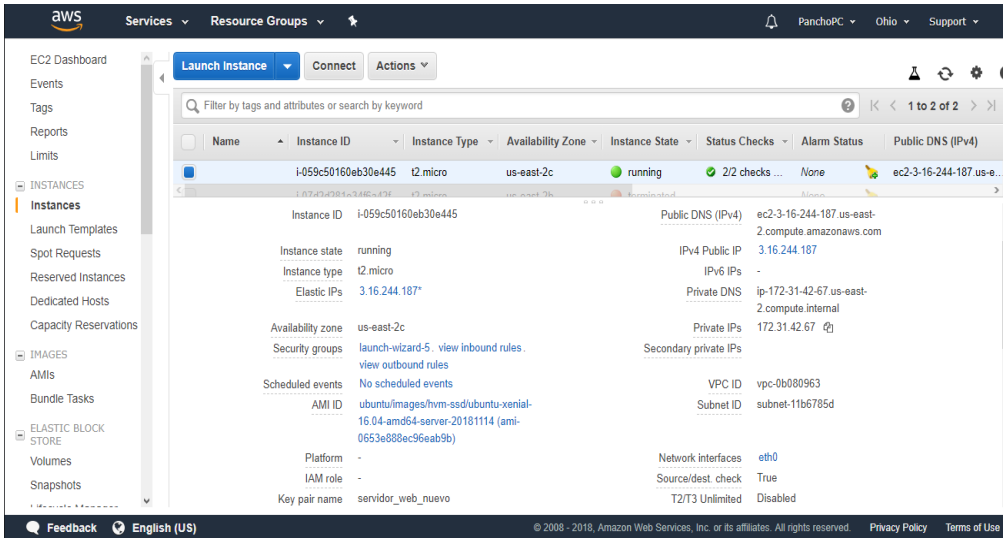

Figura 14 Instancia servidor correo creada
Elaborado: Francisco Alvear

Para que la máquina virtual pueda funcionar con salida hacia el internet se obtiene una IP pública la misma que provee Amazon. Ésta se genera automáticamente y de forma manual se asocia la IP pública con la Instancia de la máquina virtual. Teniendo así las siguientes características.

Instancia virtual AWS

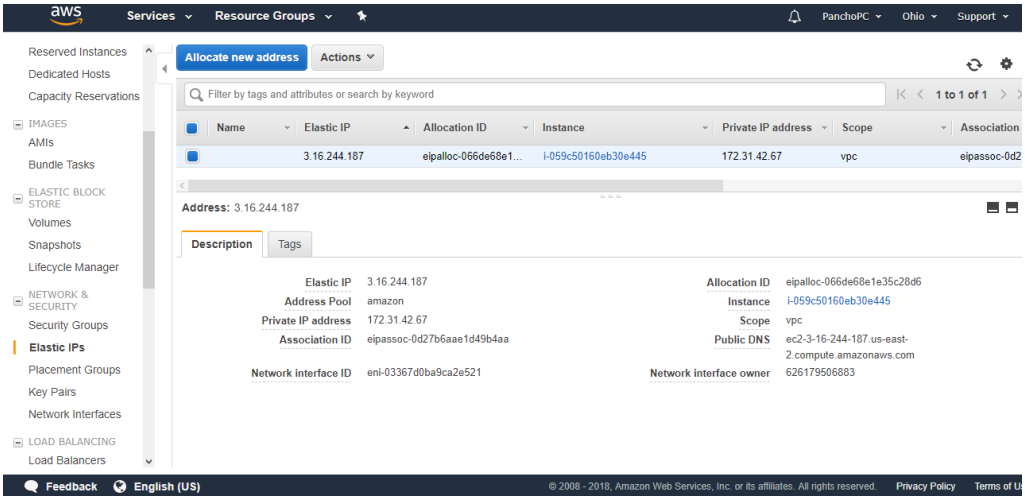

Figura 15 Características IP Pública
Elaborado: Francisco Alvear

Ya que la máquina virtual se encuentra en domino de *Amazon Web Service* se debe gestionar los permisos y los puertos que deben estar abiertos y cerrados para el manejo de los servicios en este caso se tienen los siguientes puertos abiertos.

Instancia virtual AWS

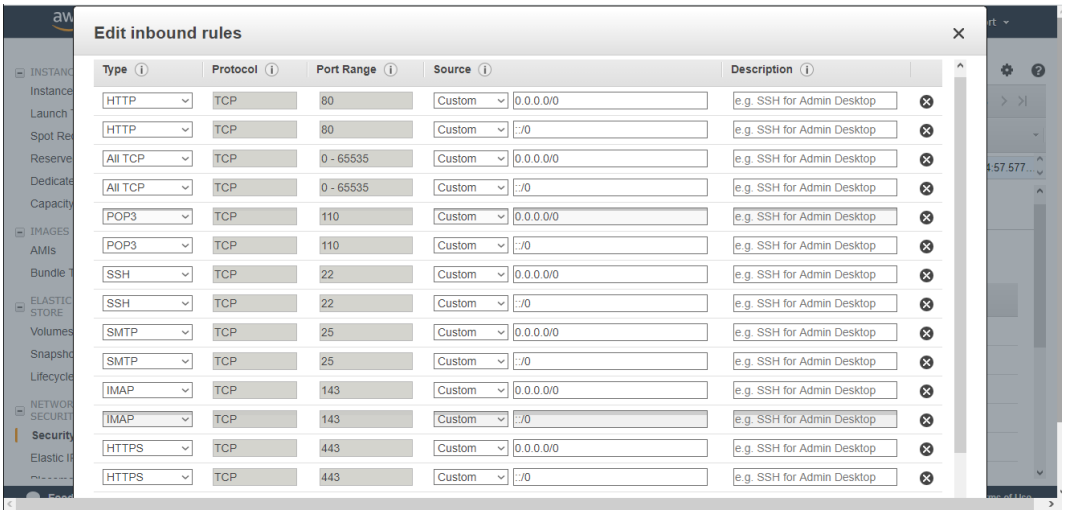

Figura 16 Puertos abiertos máquina virtual
Elaborado: Francisco Alvear

2.1.1. Configuración servidor de correo *Postfix*

2.1.1.1. Servidor *Postfix.*

Postfix es un agente de transporte de correo electrónico (MTA) que se suma a la lista de alternativas de correo electrónico de *Sendmail*, este servidor tiene varias características entre ellas: seguridad, eficiencia, facilidad de configuración en distribuciones *Linux*, administración y su ventaja especial de compatibilidad con *Sendmail* y con varios servidores de correos adicionales. El correo electrónico hoy en día es una herramienta de trabajo fundamental. *Postfix* como un sistema de correo electrónico cumple con todas las reglas con unos pocos parámetros y sin necesidad de medidas de seguridad.

2.1.1.2. Configuración servidor Postfix en Ubuntu Server

Para configurar *Ubuntu Server* se va a utilizar la herramienta PuTTY en esta herramienta se cargará la clave privada de la instancia creada en AWS, esta conexión hacia la máquina virtual se debe realizar por SSH por el puerto 22 y así tener garantizada una conexión segura hacia la máquina virtual.

Conexión instancia virtual AWS

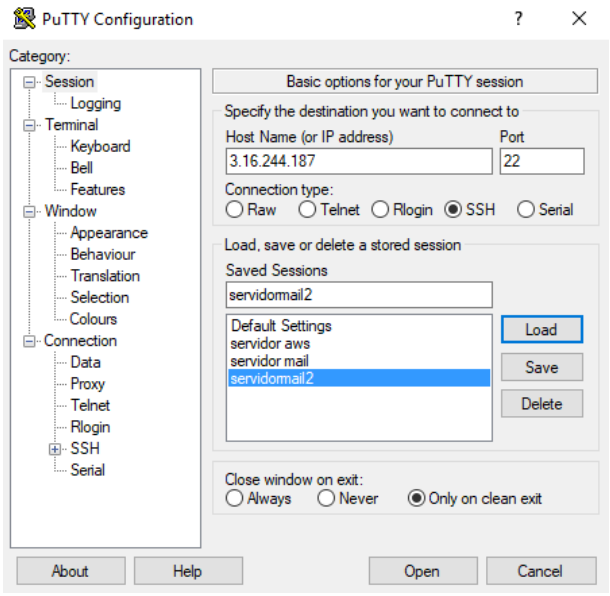

Figura 17 Conexión PuTTY máquina virtual
Elaborado: Francisco Alvear

Ingresamos como root a la consola de *Ubuntu Server* para poder realizar todas las configuraciones y levantamiento del servidor Postfix.

Conexión instancia virtual AWS

Figura 18 Modo root Ubuntu
Elaborado: Francisco Alvear

Para que no exista ningún inconveniente con los paquetes de Ubuntu se actualiza (*Update*) y mejora (*Upgrade*).

Conexión instancia virtual AWS

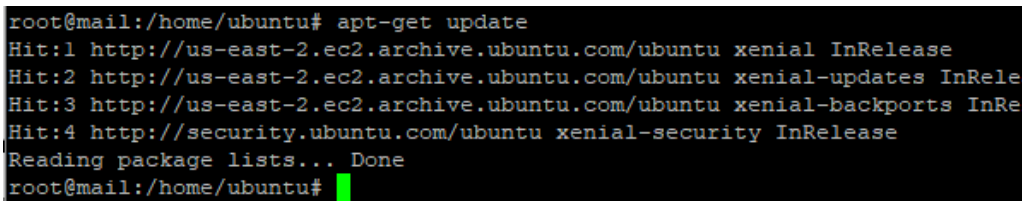

Figura 19 Actualización Ubuntu
Elaborado: Francisco Alvear

Conexión instancia virtual AWS

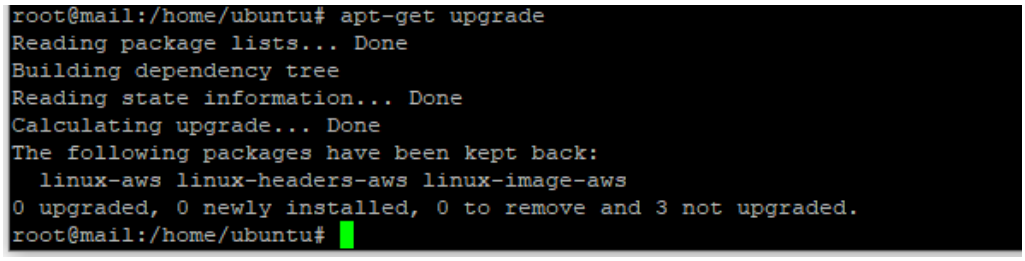

Figura 20 Upgrade Ubuntu
Elaborado: Francisco Alvear

A continuación, se instala el servidor web Apache para que aloje al servidor de correo

Conexión instancia virtual AWS

```
root@mail:/home/ubuntu# apt-get install apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
apache2 is already the newest version (2.4.18-2ubuntu3.9).
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
root@mail:/home/ubuntu#
```

Figura 21 Instalación servidor Apache en Ubuntu
Elaborado: Francisco Alvear

Se instala la herramienta mailutils que es una librería la misma que permite enviar correos electrónicos mediante la consola de Ubuntu y poder probar su correcto funcionamiento.

Conexión instancia virtual AWS

```
root@mail:/home/ubuntu# apt-get install mailutils
Reading package lists... Done
Building dependency tree
Reading state information... Done
mailutils is already the newest version (1:2.99.99-1ubuntu2).
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
root@mail:/home/ubuntu#
```

Figura 22 Instalación mailutils Ubuntu
Elaborado: Francisco Alvear

Confirmación configuración Postfix.

Conexión instancia virtual AWS

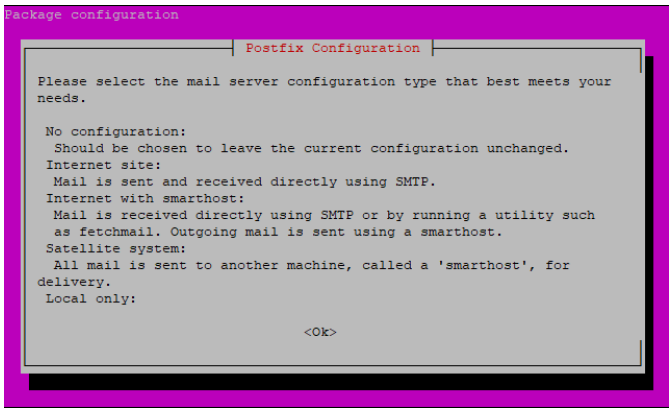

Figura 23 Instalación Postfix
Elaborado: Francisco Alvear

Configuración hacia dónde va a salir el servidor de correo electrónico.

Configuración instancia virtual AWS

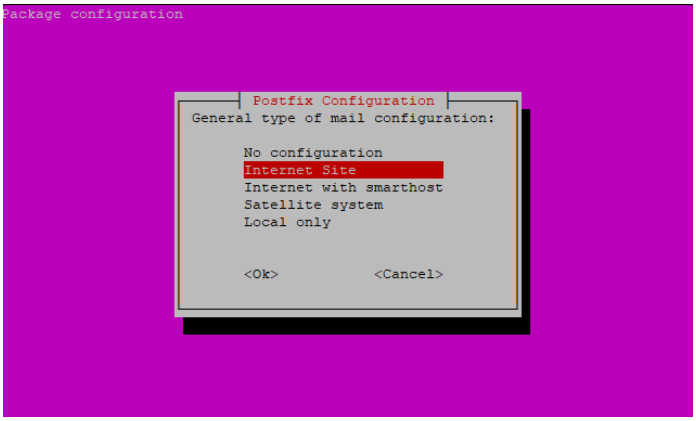

Figura 24 Instalación Postfix a Internet
Elaborado: Francisco Alvear

En este punto de configuración se coloca el dominio con el cual van a salir el correo electrónico, en este caso se utilizará "*investigacionethical.com*" y el correo tendrá la siguiente estructura: "*prueba@investigacionethical.com*".

Configuración instancia virtual AWS

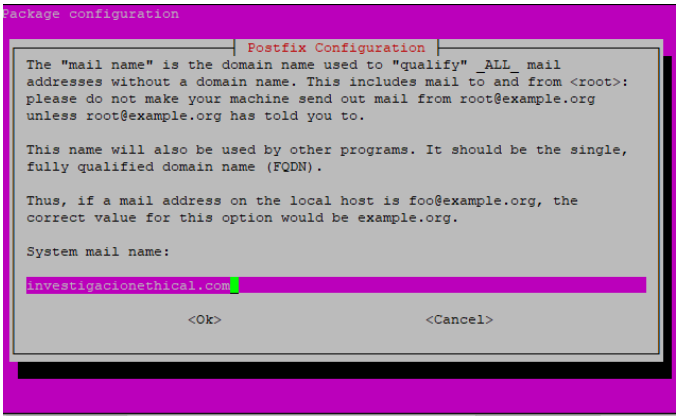

Figura 25 Configuración dominio Postfix
Elaborado: Francisco Alvear

Teniendo levantado el servidor de correo electrónico hace falta modificar archivos de configuración necesarios para que este servidor funcione correctamente primero se ingresa al archivo de configuración con el comando: *vim /etc/postfix/main.cf* en donde se edita el protocolo con el cual se va a trabajar de *all* a *ipv4* y se agrega el directorio de acceso al buzón con respecto al directorio home de cada usuario. Terminada esta configuración se reinicia el servicio con: */etc/init.d/postfix reload*

Configuración instancia virtual AWS

Figura 26 Configuración archivo Postfix
Elaborado: Francisco Alvear

Adicional se instala el servicio *courier-pop*, este servicio sirve para descargar los nuevos mensajes del servidor de correo.

Configuración instancia virtual AWS

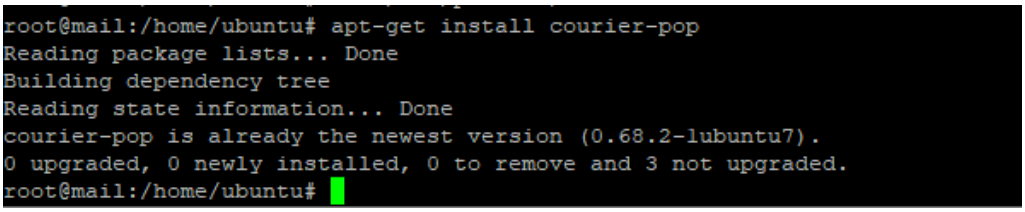

Figura 27 Instalación courier-pop Ubuntu
Elaborado: Francisco Alvear

Configuración instancia virtual AWS

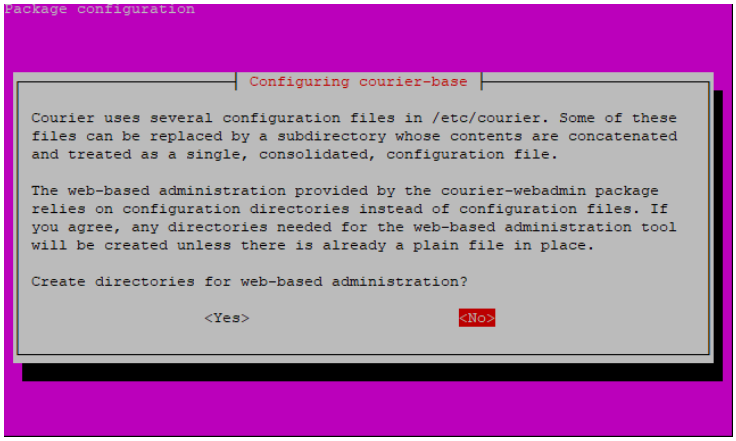

Figura 28 Configuración base de datos Courier
Elaborado: Francisco Alvear

A continuación, se instala el protocolo imap el mismo que permite que desde cualquier dispositivo se pueda ingresar al servidor de correo.

Configuración instancia virtual AWS

```
root@mail:/home/ubuntu# apt-get install courier-imap
Reading package lists... Done
Building dependency tree
Reading state information... Done
courier-imap is already the newest version (4.10.0-20120615-1ubuntu7).
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
root@mail:/home/ubuntu#
```

Figura 29 Instalación courier-imap Ubuntu
Elaborado: Francisco Alvear

Para el servidor de correo electrónico es necesario una interfaz gráfica amigable para el usuario final, para esto se va a instalar el servicio de Squirrelmail que es una aplicación web gratuita que permite visualizar los correos enviados y recibidos de los usuarios.

Configuración instancia virtual AWS

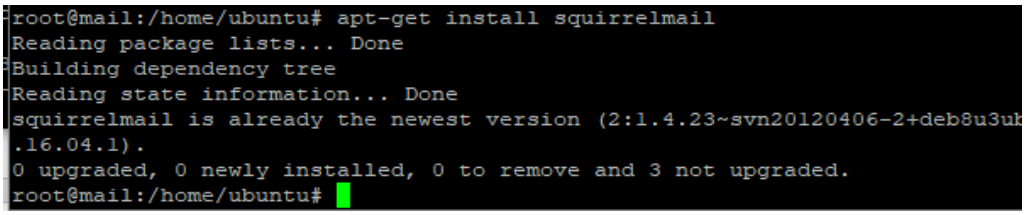

Figura 30 Instalación squirrelmail Ubuntu
Elaborado: Francisco Alvear

Ya que la interfaz gráfica Squirrelmail está instalada se configura con el comando: *squirrelmail-configure.*

Configuración instancia virtual AWS

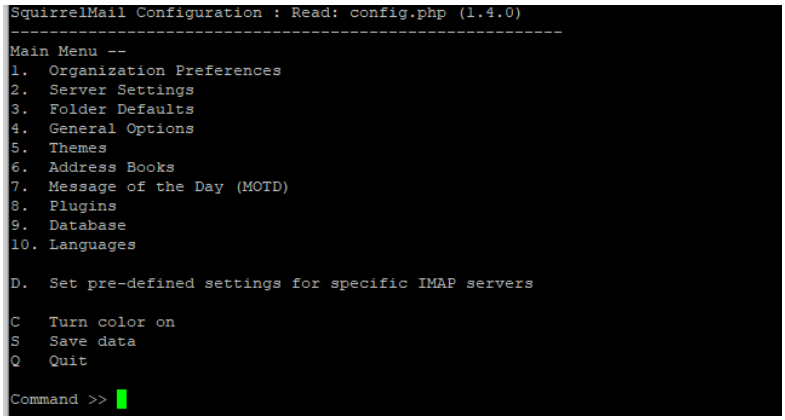

Figura 31 Configuración squirrelmail
Elaborado: Francisco Alvear

Se configura IMAP servers con la letra D y al configurar IMAP elegimos el servidor courier.

Configuración instancia virtual AWS

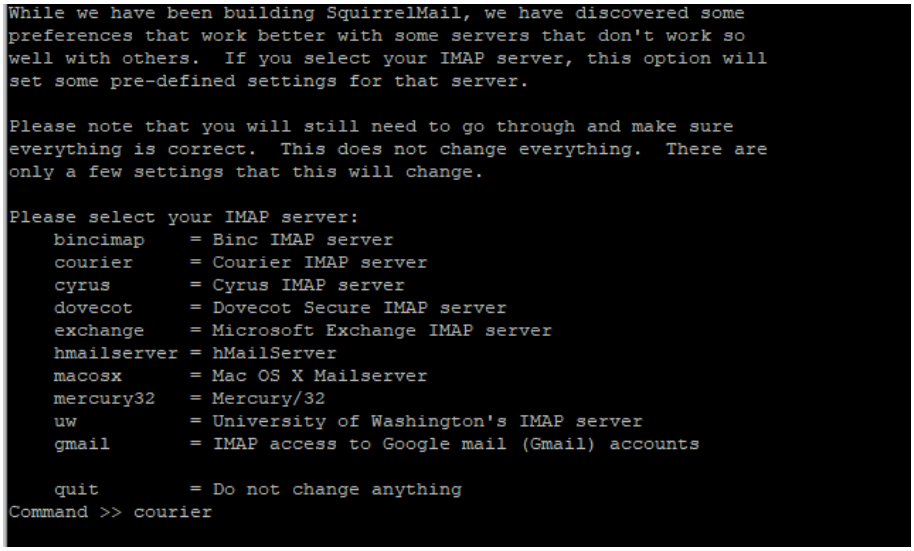

Figura 32 Configuración IMAP Courier
Elaborado: Francisco Alvear

Se elige la configuración del servidor con la opción 2

Configuración instancia virtual AWS

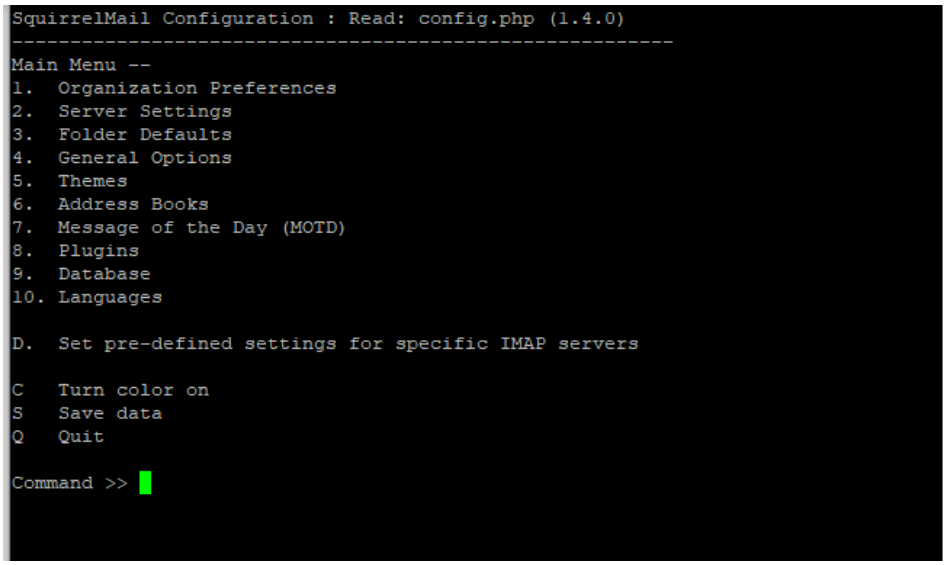

Figura 33 Configuración servidor Courier
Elaborado: Francisco Alvear

Se verifica el dominio con el que va a funcional el servidor de correo tanto para él envió de correo electrónico como para que puedan regresar las respuestas de estos.

Configuración instancia virtual AWS

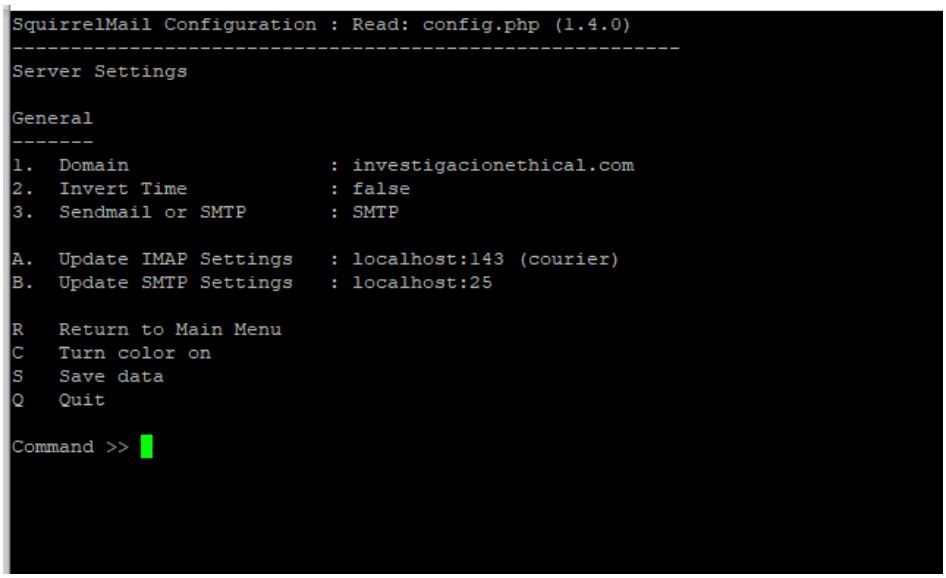

Figura 34 Verificación de dominio Squirrelmail
Elaborado: Francisco Alvear

Después de esta configuración en Squirrelmail lo siguiente en realizar es la creación en el directorio root de apache un acceso directo a la dirección de Squirrelmail con el siguiente comando:

Configuración instancia virtual AWS

Figura 35 Acceso directo servidor webmail
Elaborado: Francisco Alvear

En esta instancia se modificará el archivo de configuración de apache para definir qué es lo que se va a presentar al momento de ingresar la url en el navegador para esto se usa el comando: *vim /etc/apache2/sites-available/000-default.conf* donde se refleja el

siguiente archivo en el que se verifica la url a la que se redirige al momento de llamar al servidor web. Verificado la ruta del servidor web reiniciamos el servicio con el comando: */etc/init.d/apache2 restart*.

Configuración instancia virtual AWS

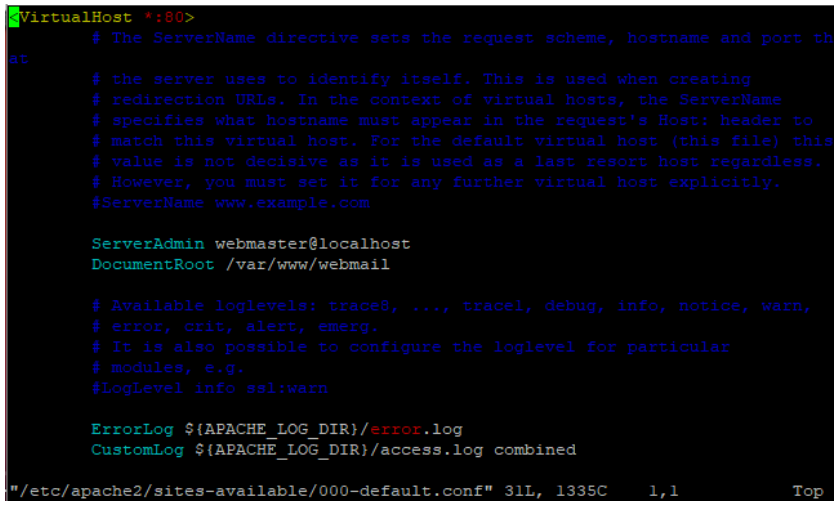

Figura 36 Archivo de configuración apache2
Elaborado: Francisco Alvear

Se crea un usuario con el comando: *adduser tesis2* y se pedirá varios datos como contraseña, nombres, teléfono oficina, teléfono casa y un campo otro en el cual se puede escribir una observación sobre el usuario creado.

Configuración instancia virtual AWS

```
root@mail:/home/ubuntu# adduser tesis2
Adding user `tesis2' ...
Adding new group `tesis2' (1006) ...
Adding new user `tesis2' (1006) with group `tesis2' ...
Creating home directory `/home/tesis2' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for tesis2
Enter the new value, or press ENTER for the default
        Full Name []: Francisco Alvear
        Room Number []: 66
        Work Phone []: 2974959
        Home Phone []: 2974959
        Other []: Usuario creado pruebas servidor de correo
Is the information correct? [Y/n] y
root@mail:/home/ubuntu#
```

Figura 37 Creación usuario correo
Elaborado: Francisco Alvear

Se crea un servicio demonio para que pueda inicializar el servicio courier inmediatamente se prenda la instancia virtual para esto se escribe el siguiente comando: *systemctl enable courier-authdaemon* creado este servicio se procede a ejecutar con el siguiente comando: *service courier-authdaemon start* y para que estas configuraciones se hagan efectivas se reinicia la instancia con: *reboot.*

Configuración instancia virtual AWS

```
root@mail:/home/ubuntu# systemctl enable courier-authdaemon
Synchronizing state of courier-authdaemon.service with SysV init with /lib/
md/systemd-sysv-install...
Executing /lib/systemd/systemd-sysv-install enable courier-authdaemon
root@mail:/home/ubuntu# service courier-athdaemon start
Failed to start courier-athdaemon.service: Unit courier-athdaemon.service n
und.
root@mail:/home/ubuntu# service courier-authdaemon start
root@mail:/home/ubuntu# reboot
```

Figura 38 Configuración inicio de servicio Courier
Elaborado: Francisco Alvear

2.1.1.3. Configuración servidor DNS Route 53 Amazon Web Service

Para poder registrar un dominio *Amazon Web Service* ofrece la herramienta *Route* 53 en donde se puede elegir un nombre de dominio que en este caso es: investigacionethical.com, ya obtenido el nombre de dominio hay que configurar en esta herramienta a que IP pública va a apuntar este nombre de dominio.

Para esto se configura una zona A con que apunta a la dirección IP pública de la instancia virtual que en este caso la IP pública es: 3.16.244.187.

Configuración DNS en AWS

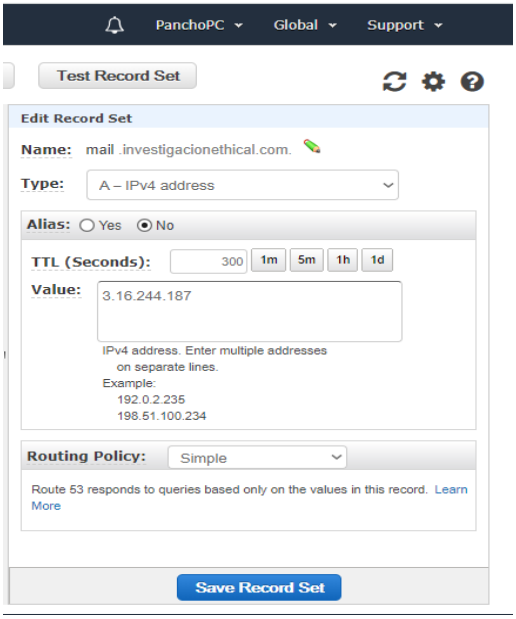

Figura 39 Creación tipo A Route 53
Elaborado: Francisco Alvear

Para que los servidores de correo electrónicos como Gmail, Hotmail u otro servidor de correo sepan a qué dirección deben responder se creó un registro MX de correo, esto se crea dentro del servidor DNS público que está disponible para todo el internet.

Configuración DNS en AWS

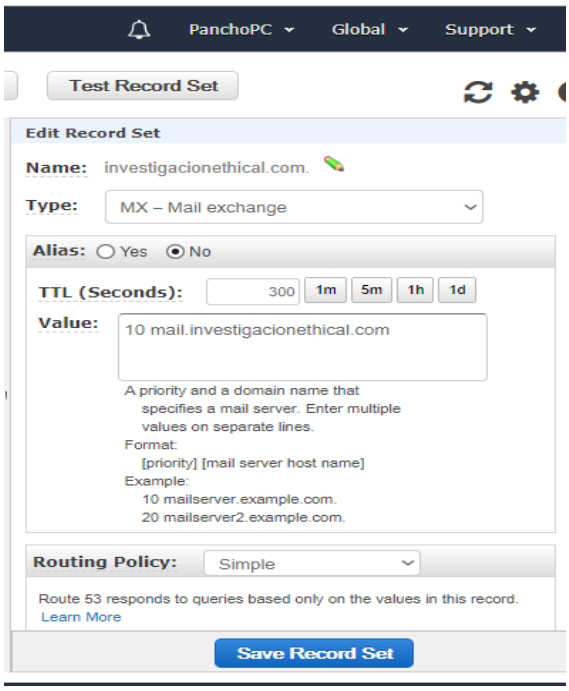

Figura 40 Configuración registro MX correo
Elaborado: Francisco Alvear

Y es así como queda la tabla del servidor DNS con los registros creados para el servidor de correo junto a los servidores DNS públicos de *Amazon Web Service*.

Configuración DNS en AWS

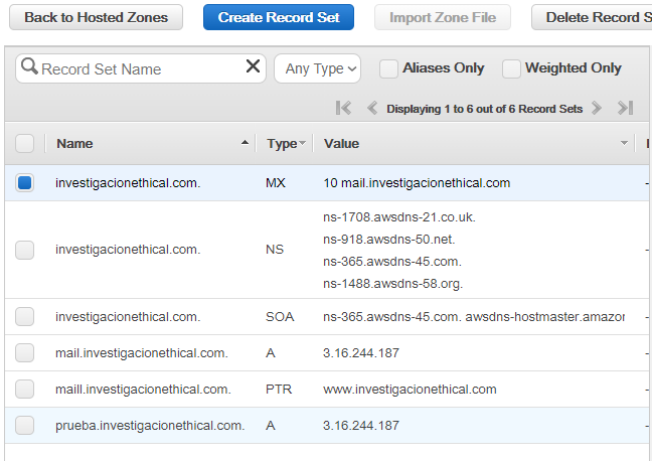

Figura 41 Tabla de direcciones DNS
Elaborado: Francisco Alvear

2.1.1.4. Pruebas servidor de correo electrónico

En las pruebas de servidor de correo electrónico se ingresa al navegador de preferencia y con la url: mail.investigacionethical.com nos redirige al servidor de correo.

Pruebas servidor de correo electrónico

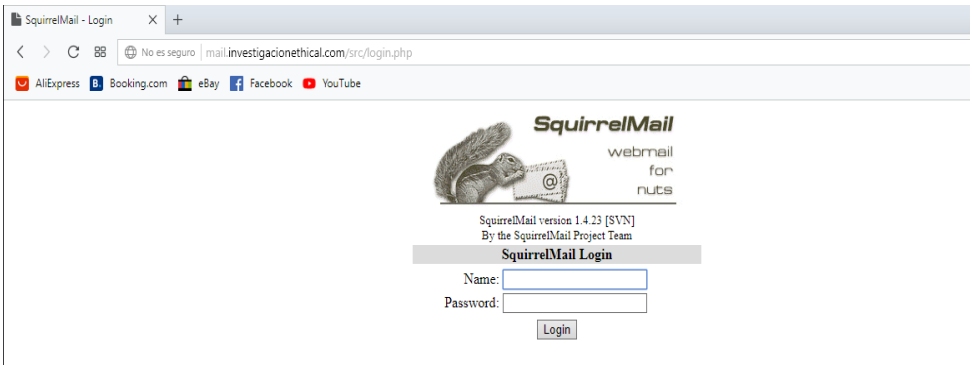

Figura 42 Servidor de correo en navegador
Elaborado: Francisco Alvear

Se ingresa con el usuario tesis2@investigacionethical.com que se creó anteriormente para pruebas de envío y recepción de mails.

Pruebas servidor de correo electrónico

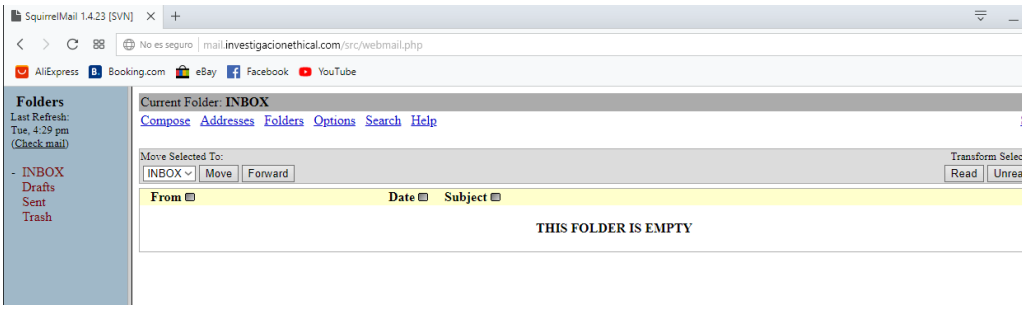

Figura 43 Interfaz servidor de correo
Elaborado: Francisco Alvear

La prueba del servidor de correo es hacia un correo Gmail el mismo que se llegará a verificar el envío de éste.

Pruebas servidor de correo electrónico

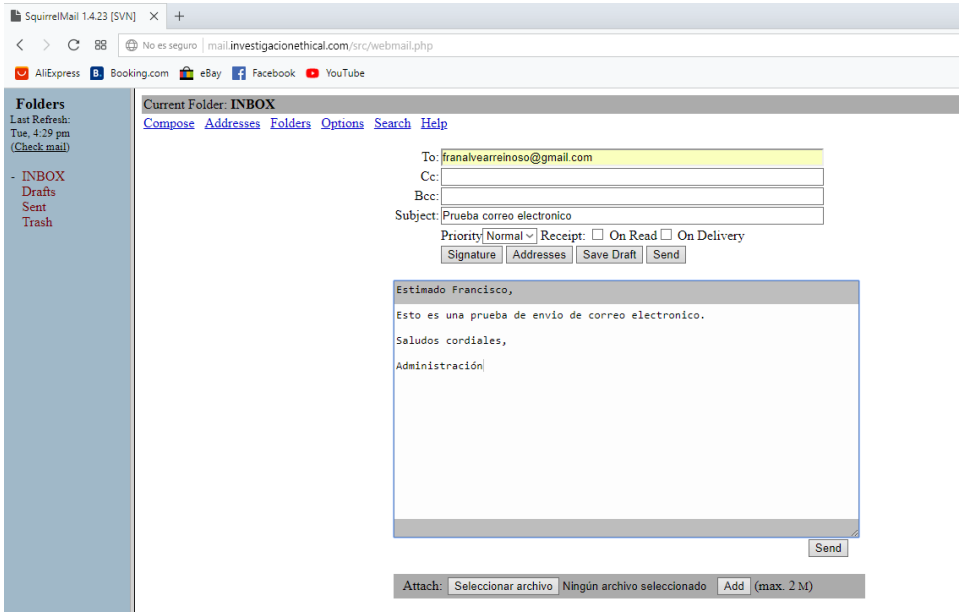

Figura 44 Envió de correo electrónico
Elaborado: Francisco Alvear

Pruebas servidor de correo electrónico

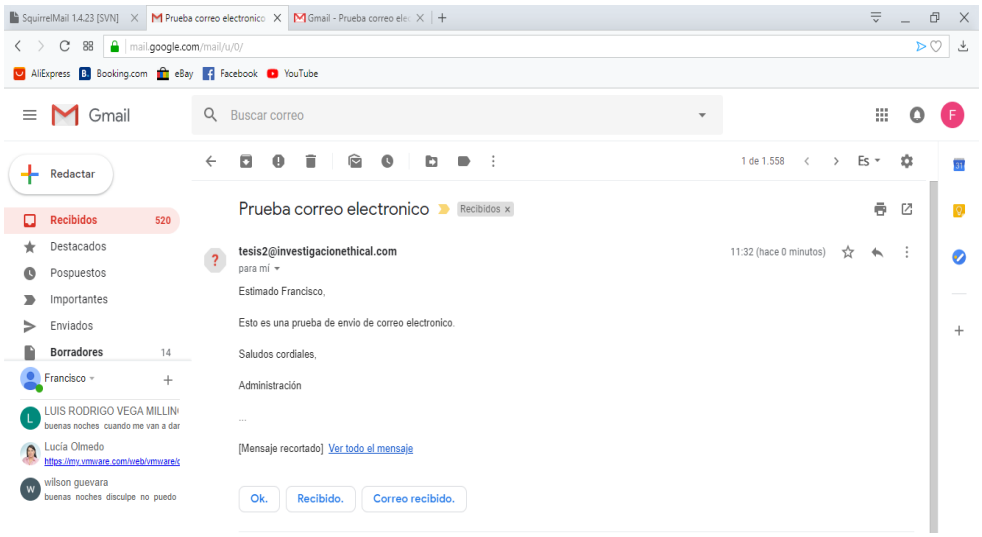

Figura 45 Correo recibido en Gmail
Elaborado: Francisco Alvear

Para la respuesta desde el servidor de correo Gmail, este servidor busca el registro MX del servidor de donde fue enviado para poder responder y como respuesta tenemos que si llega el correo electrónico desde Gmail hasta el servidor Postfix.

Configuración instancia virtual AWS

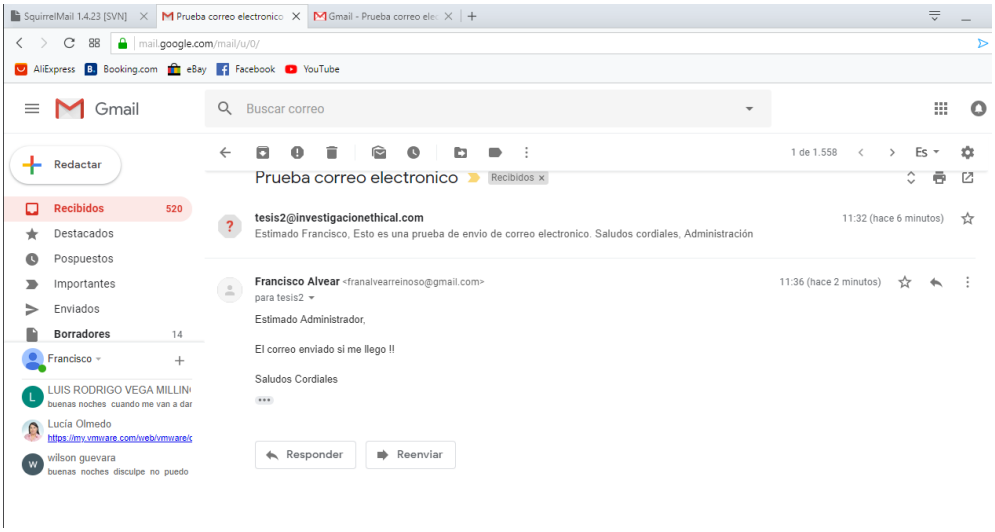

Figura 46 Respuesta servidor Gmail
Elaborado: Francisco Alvear

Configuración instancia virtual AWS

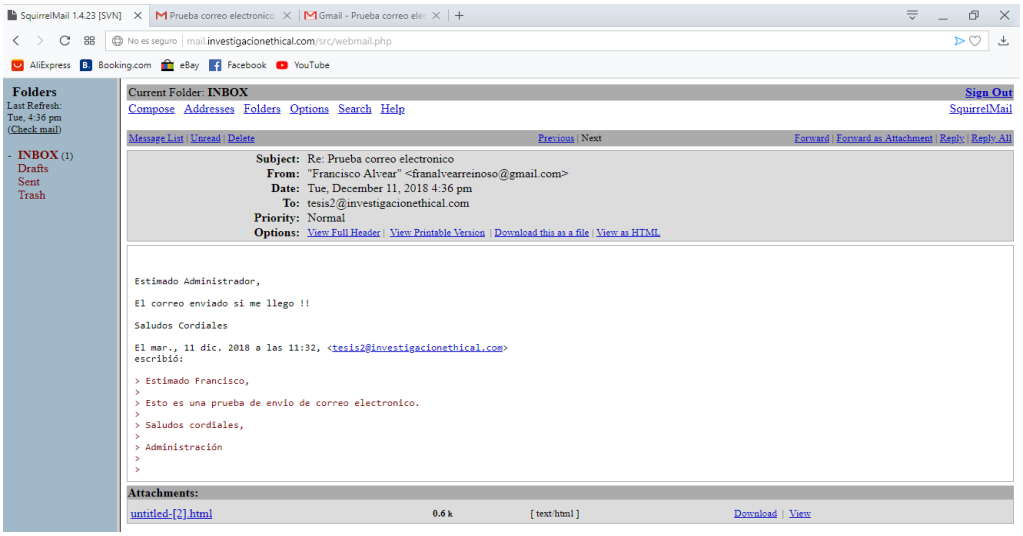

Figura 47 Respuesta servidor Postfix
Elaborado: Francisco Alvear

2.1.2. Ataques reales a correo electrónico

2.1.2.1. Ataque Spoofing

El ataque de *Spoofing* se realiza desde el mismo servidor de correo, en este servidor primero se instala el servicio PHP para que pueda ejecutar el archivo y realizar este tipo de ataque.

Instalar servicio php en Ubuntu server

Ataque de Spoofing

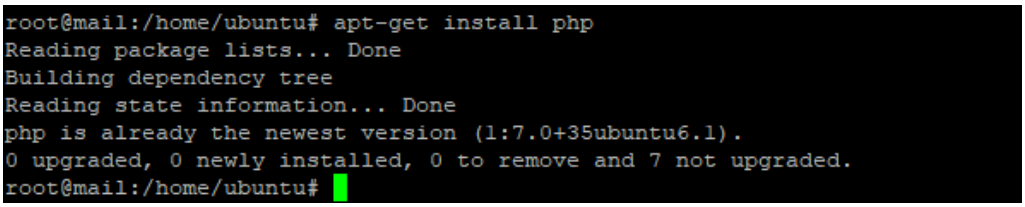

Figura 48 Instalación php Ubuntu
Elaborado: Francisco Alvear

Se crea una carpeta dentro del servidor apache 2 con nombre prueba, en esta carpeta se crea el archivo correo.php con el siguiente contenido

Código ataque de Spoofing

```
<?php
$to=  "franalvearreinoso@gmail.com";   Email de la víctima
$subject = "Ganaste la Loteria" ;                Asunto del email
$message = "Actualiza tus datos";                Mensaje
$from = fausto.alvear@cefoseg.edu.ec                Cuenta suplantada
$headers = "From:" .$from;                       De
$mail = mail($to,$subject,$message,$headers,$from);   Método de suplantación
if($mail)
{
echo "Email sent to" .$to;
}
?>
```

Figura 49 Código PHP spoofing
Elaborado: Francisco Alvear

Al ejecutar este código php regresa como mensaje: Mail enviado a correo@gmail.com

Código ataque de Spoofing

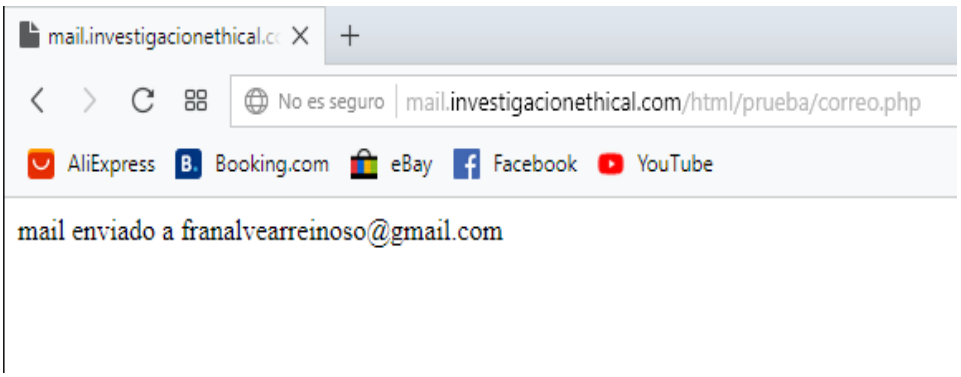

Figura 50 Spoofing enviado
Elaborado: Francisco Alvear

El correo recibido llega a la bandeja de entrada directamente con el correo www-

data@investigacionethical.com el mismo que evita que este tipo de ataque no se realice con fines malignos sino como prueba de hacking ético.

Ataque de Spoofing

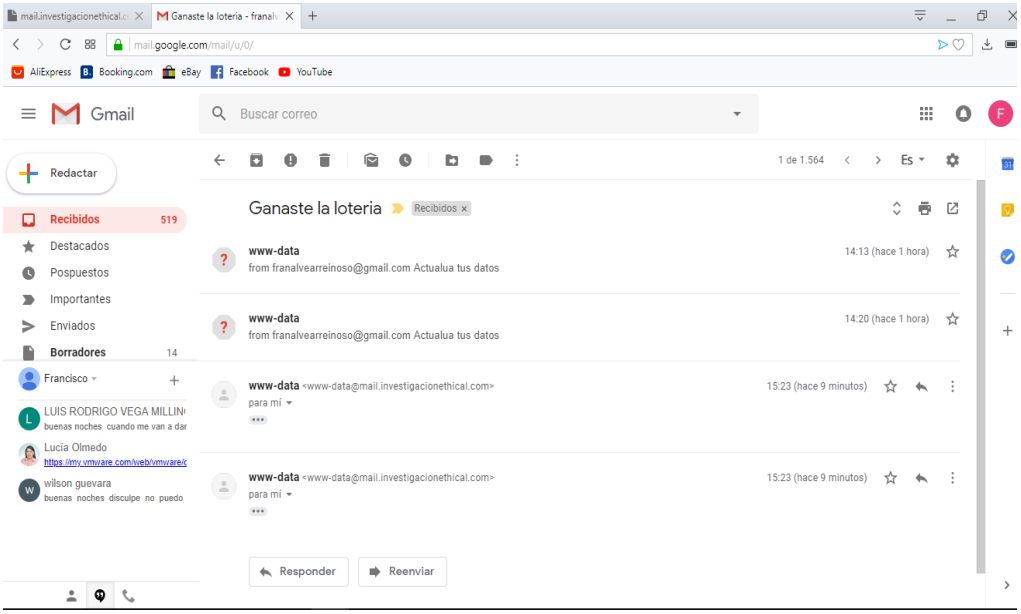

Figura 51 Mail con spoofing
Elaborado: Francisco Alvear

2.1.2.2. Ataque Phishing

Para el ataque de *Phishing* que se realizó a diferentes usuarios por medio de correo electrónico se implementó una instancia virtual en *Amazon Web Service* la misma que tiene como dirección IP pública 18.223.105.221, en esta instancia virtual se instaló el programa SET (*The Social-Engineer Toolkit*), esta herramienta de software libre está programada en *Python*.

Para su descarga se clona desde la página de *github*, en la instancia virtual se instala todos los requisitos que necesita esta herramienta para poder ejecutarse con éxito. A continuación, se detallan los comandos ejecutados.

Ataque de Phishing

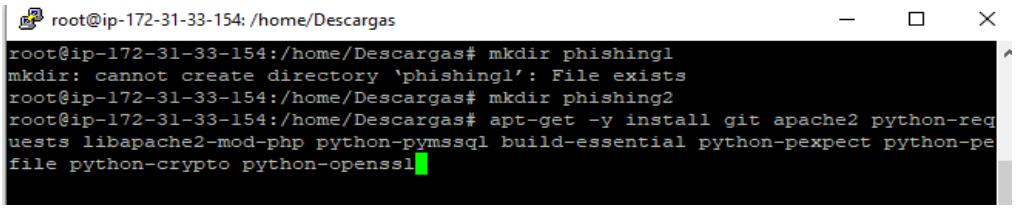

Figura 52 Comando instalación php
Elaborado: Francisco Alvear

Ya instalado los requerimientos para que pueda ejecutar la herramienta SET se debe clonar los archivos de la herramienta desde *GitHub* con el siguiente comando.

Ataque de Phishing

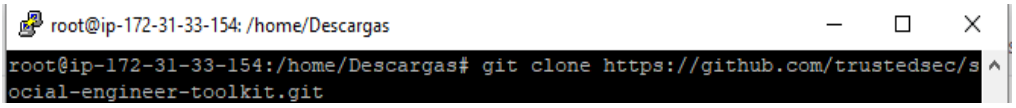

Figura 53 Descarga herramineta SET
Elaborado: Francisco Alvear

Verificamos que se copió la carpeta social-engineer-toolkit, dentro de esta carpeta tenemos los siguientes archivos.

Ataque de Phishing

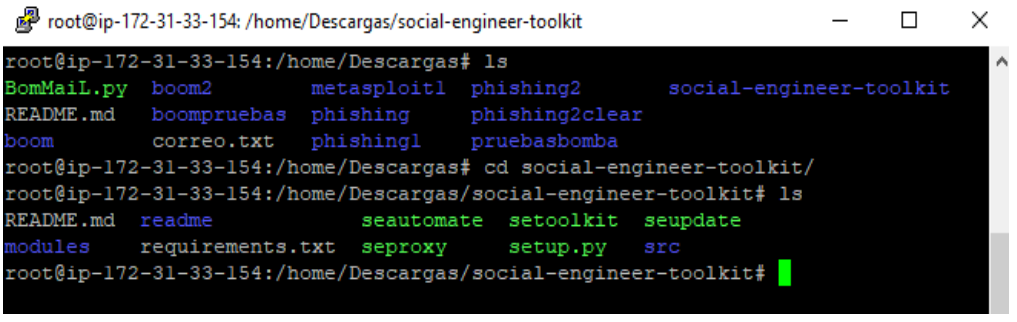

Figura 54 Archivos herramienta SET
Elaborado: Francisco Alvear

Al ejecutar el archivo *setoolkit* con el comando *./setoolkit*, se puede reflejar el menú en el cual se puede escoger una serie de opciones para realizar hacking ético.

Ataque de Phishing

Figura 55 Interfaz SET
Elaborado: Francisco Alvear

En este menú se escoge la opción 1 Ataque de Ingeniería Social, la herramienta presenta un nuevo menú.

Ataque de Phishing

Figura 56 Interfaz Ataque Ingeniería Social
Elaborado: Francisco Alvear

En este menú se elige la segunda opción Ataque de sitio Web, en el cual presenta el siguiente menú.

Ataque de Phishing

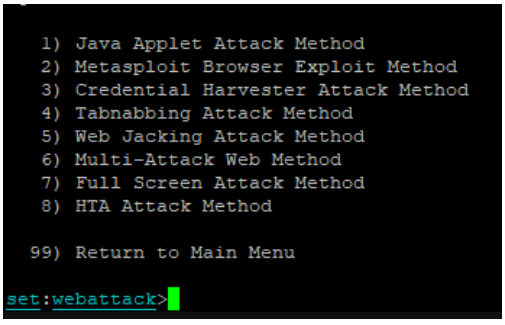

Figura 57 Menú Ataque de Sitio Web
Elaborado: Francisco Alvear

En el siguiente menú se elige la opción 3, en este método existen tres opciones para la creación del sitio web falso, en este caso se clonará una página web.

Ataque de Phishing

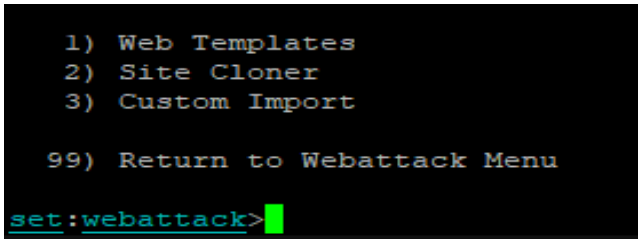

Figura 58 Menú métodos de clonación página web
Elaborado: Francisco Alvear

Se elige la opción 2 en el cual se clonará una página web, en este caso se clonará el login de Facebook.

Ataque de Phishing

Figura 59 Clonación página web Facebook
Elaborado: Francisco Alvear

Para poder completar la clonación de la página web de Facebook la herramienta pide la IP en la cual se encuentra alojado el servidor web para poder ejecutar la página clonada y adicional cual es el sitio web que se va a clonar, en este caso como IP de servidor se coloca la IP pública del servidor para que sea visible por todos los usuarios (18.223.105.221) y el sitio web: www.facebook.com.

Para que este ataque sea satisfactorio no se puede entregar a la víctima una IP pública porque no podría caer en la trampa, para esto dentro de dominio investigacionethical.com creamos un registro A con www.facebook.investigacionethical.com para así poder disfrazar este tipo de ataque. Este registro apunta a la dirección de IP pública de la Instancia virtual.

Ataque de Phishing

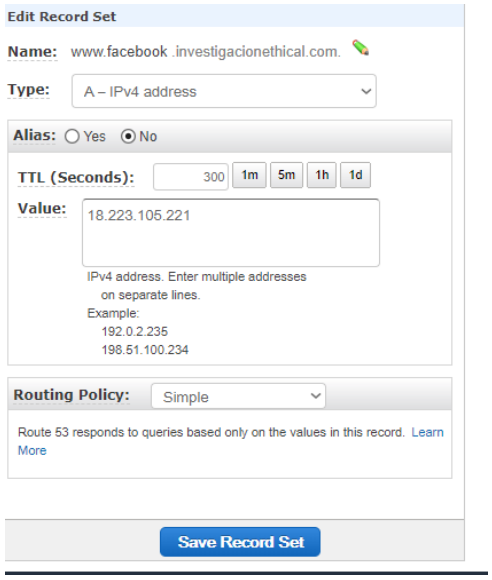

Figura 60 Registro A página clonada de Facebook
Elaborado: Francisco Alvear

De esta manera este tipo de ataque tiene una eficacia mayor ya que el URL es idéntico al de Facebook original, este ataque se lo realizó mediante correo electrónico enviando a la víctima una imagen de Facebook advirtiendo el inicio de sesión fallido en su cuenta personal.

Se utilizó el ataque de *Spoofing* para poder enviar un correo que dentro del mismo lleva una imagen con el link a la página falsa de Facebook. El código utilizado para este ataque es:

Ataque de Phishing

```
<?php

$to  = 'test-r1wui@mail-tester.com' . ', '; // note the comma
$to .= '';
$subject = 'Inicio de sesión fallido';
$message = '
<html>
<head>
  <meta http-equiv="Content-Type" content="text/html; charset="UTF-8" />
</head>
<body>
  <p>Se ha detectado un inicio de sesión fallido</p>
  <a href="http://www.facebook.investigacionethical.com"><img src="https://pepepancho1234.000webhostapp.com/prueba.jpg" /> </a>
  </table>
</body>
</html>
';
$headers  = 'MIME-Version: 1.0' . "\r\n";
$headers .= 'Content-type: text/html; charset=UTF-8' . "\r\n";
$headers .= 'To: <test-r1wui@mail-tester.com>' . "\r\n";
$headers .= 'From: Inicio de sesión fallido <soportefacebook@facebok.com>' . "\r\n";
$headers .= 'Cc: ' . "\r\n";
// Mail it
mail($to, $subject, $message, $headers);
echo  "Email sent to" .$to;
?>
```

Figura 61 Código de ataque Spoofing
Elaborado: Francisco Alvear

Al ejecutar el archivo correo.php se muestra el siguiente mensaje confirmando el envío del correo electrónico a la víctima.

Ataque de Phishing

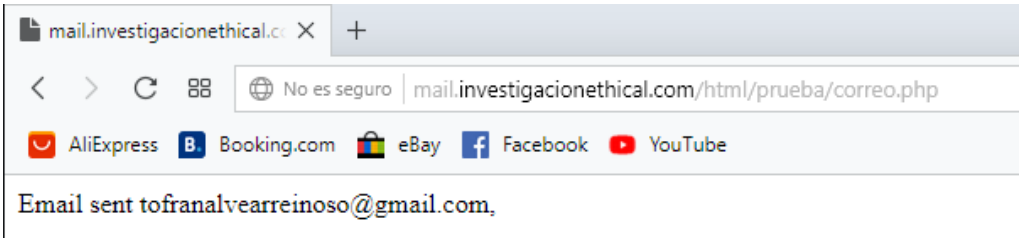

Figura 63 Envío spoofing con pishing
Elaborado: Francisco Alvear

El correo que llega a la víctima esta con el nombre de "Inicio de sesión fallido" enviado por el correo soportefacebook@facebok.com dentro del correo la imagen de advertencia de Facebook.

Ataque de Phishing

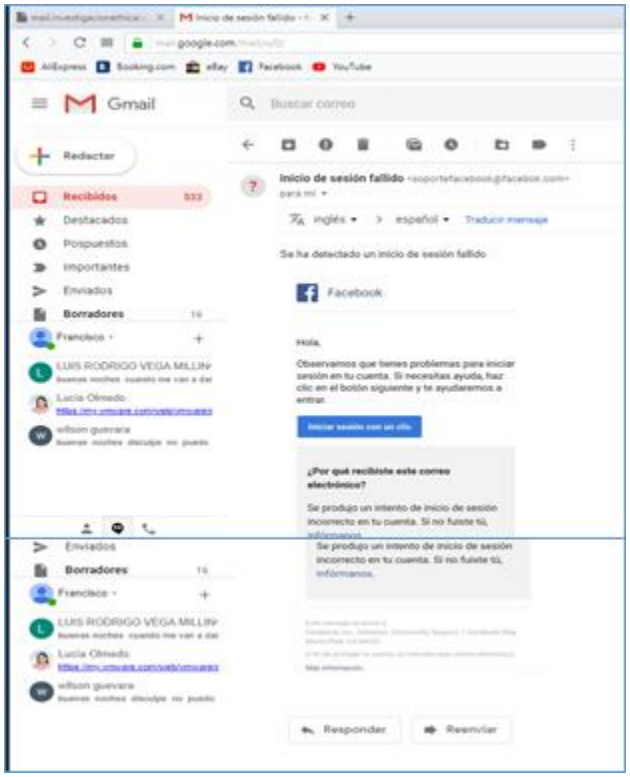

Figura 64 Correo en mail de victima
Elaborado: Francisco Alvear

Al dar click sobre la imagen en el correo electrónico se redirige a la URL www.facebook.investigacionethical.com en el cual se encuentra la página duplicada de Facebook.

Ataque de Phishing

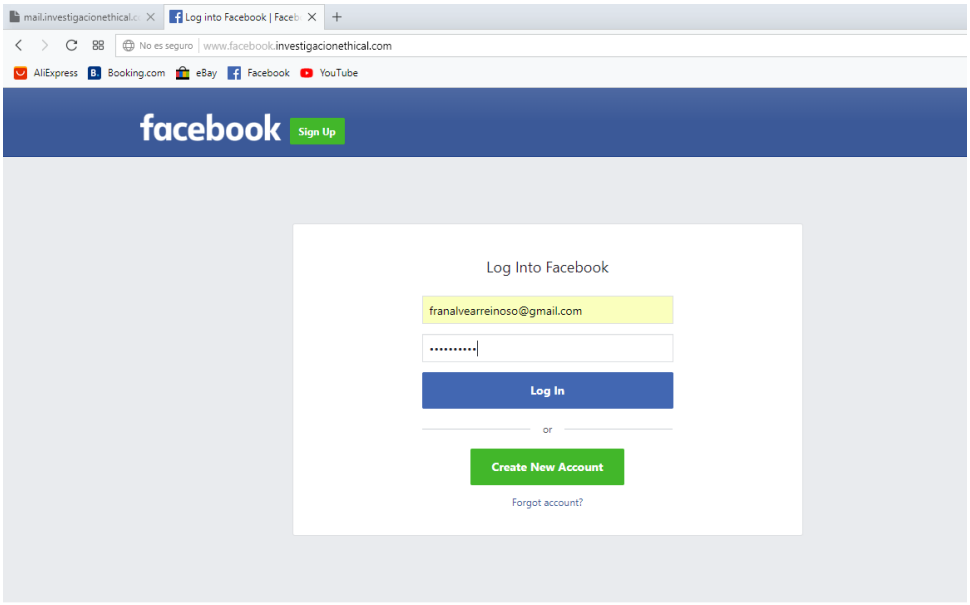

Figura 65 Página clonada de Facebook
Elaborado: Francisco Alvear

En la página clonada de Facebook ingresamos el correo electrónico franalvearreinoso@gmail.com junto con la clave “Pancho1805”, al dar click en Log In se envían los datos ingresados en correo y contraseña a la instancia virtual que se mantiene en escucha con la IP pública.

En la instancia virtual se refleja los siguientes resultados:

Ataque de Phishing

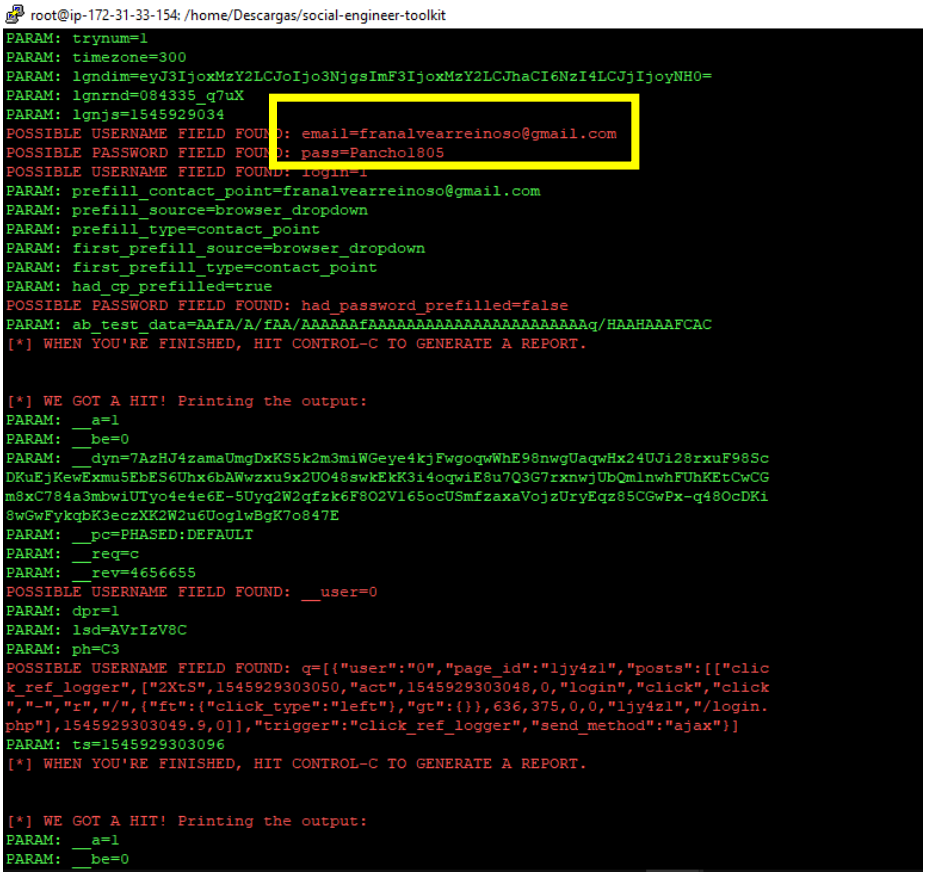

Figura 66 Datos obtenidos en Instancia virtual
Elaborado: Francisco Alvear

De esta manera se puede llegar a obtener información importante de las víctimas por medio de *phishing*, este tipo de ataque está orientado a obtener información relevante de las víctimas, pero sobre todo buscan obtener información financiera para posibles robos con los datos de tarjetas de crédito.

2.1.2.3. Ataque de Mailing

En este tipo de ataque se puede enviar a un número grande usuarios un correo individual utilizando la herramienta SET, el correo que se va a enviar contiene el ataque de *phishing* el mismo que se lo explicó anteriormente. Para esto se debe ejecutar la herramienta *Setoolkit* y se elige la opción 1.

Ataque de Mailing

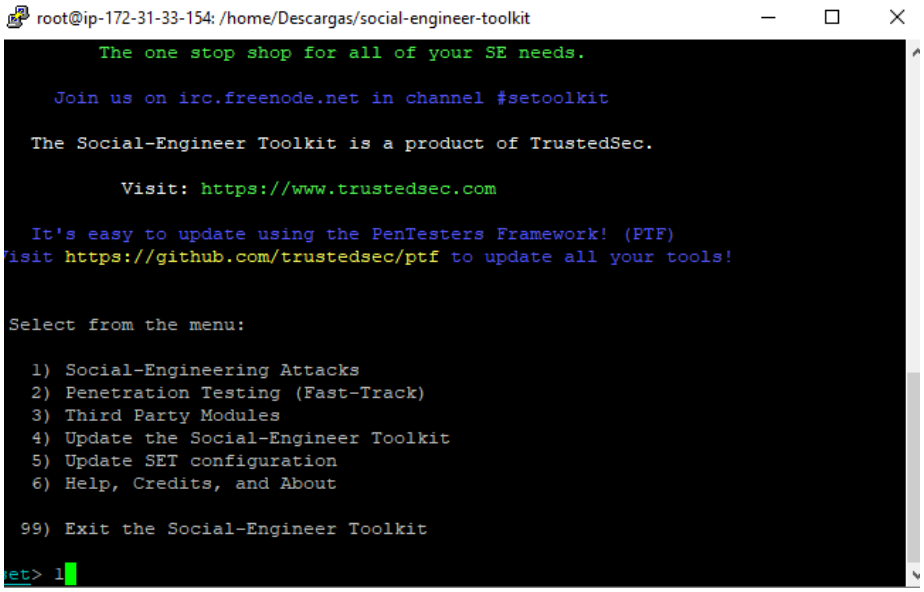

Figura 67 Menu Setoolkit
Elaborado: Francisco Alvear

En el menú de ataque de Ingeniería Social se escoge la opción 5 ataque de mail masivo, el mismo que se utilizó para enviar una serie de correos con el ataque.

Ataque de Mailing

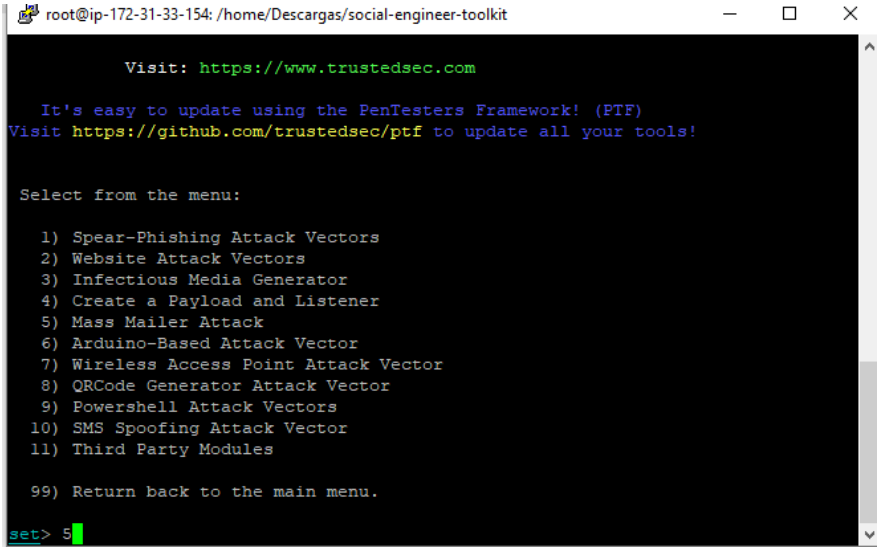

Figura 68 Menú ataque de correo masivo
Elaborado: Francisco Alvear

Se elige la opción 2 en la cual vamos a utilizar un archivo .txt en el cual se tiene todos los correos electrónicos a los cuales van a ser enviados este ataque, para esto se debe incluir la dirección donde se encuentra el archivo de texto con los correos electrónicos.

Ataque de Mailing

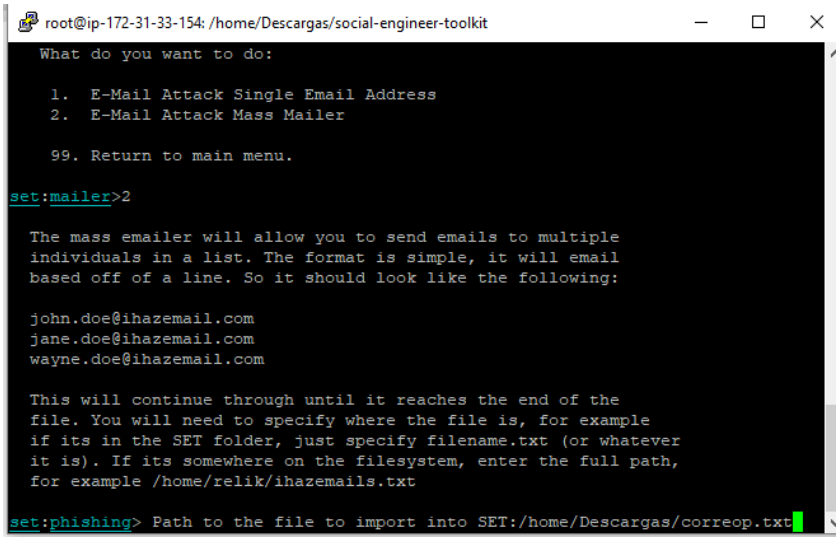

Figura 69 Dirección de archivo de texto con correos
Elaborado: Francisco Alvear

El archivo correop.txt contiene los siguientes correos electrónicos los mismos que serán verificados que se envíe el ataque con *phishing.*

Ataque de Mailing

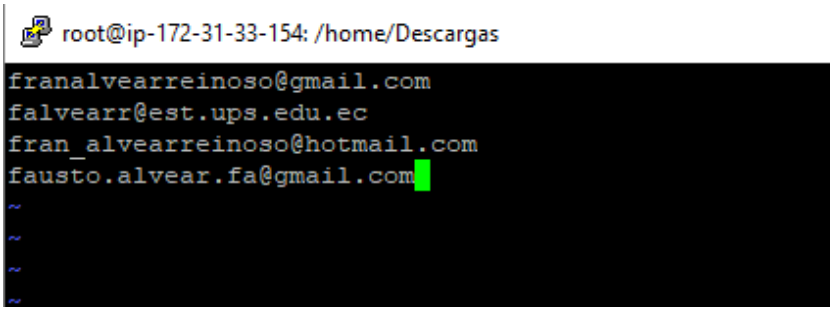

Figura 70 Archivo con correo electrónicos
Elaborado: Francisco Alvear

Elegimos la opción 1 en la cual se utiliza un correo electrónico de Gmail creado anteriormente, este correo electrónico será remplazado por la frase “Intento de sesión fallido” y SET ingresa al correo de Gmail ingresando la clave que se coloca, pregunta si el correo enviado tiene una prioridad alta y se coloca YES, no se adjunta archivos al correo, como Asunto del correo se coloca “Inicio de sesión bloqueado” y se envía un correo electrónico en formato HTML el mismo que se detalla:

Ataque de Mailing

Hola, fue victima de un inicio de sesión fallido

Ingrese a este link para poder restablecer su cuenta de Facebook http://www.facebook.investigacionethical.com

Ingrese al botón Iniciar sesión con un click del mensaje

Si tiene alguna duda o sugerencia contactarse al correo soportefacebook@investigacionethical.com

END

Figura 71 Correo electrónico en formato HTML. Ataque de Phishing
Elaborado: Francisco Alvear

Ya enviado este mensaje tenemos la confirmación del envío del correo electrónico a los usuarios del archivo .txt

Ataque de Mailing

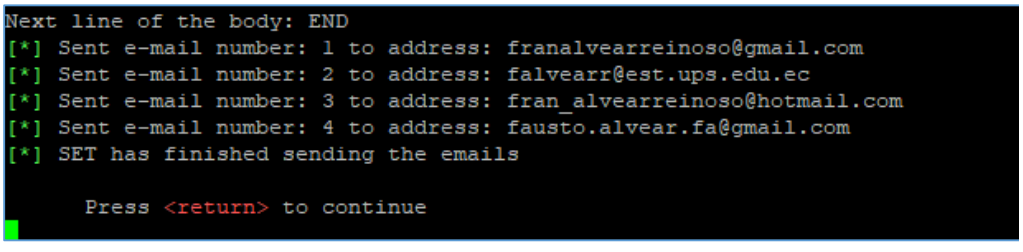

Figura 73 Confirmación de correo electrónico
Elaborado: Francisco Alvear

Correo que llegó a la víctima en diferentes servidores.

Ataque de Mailing

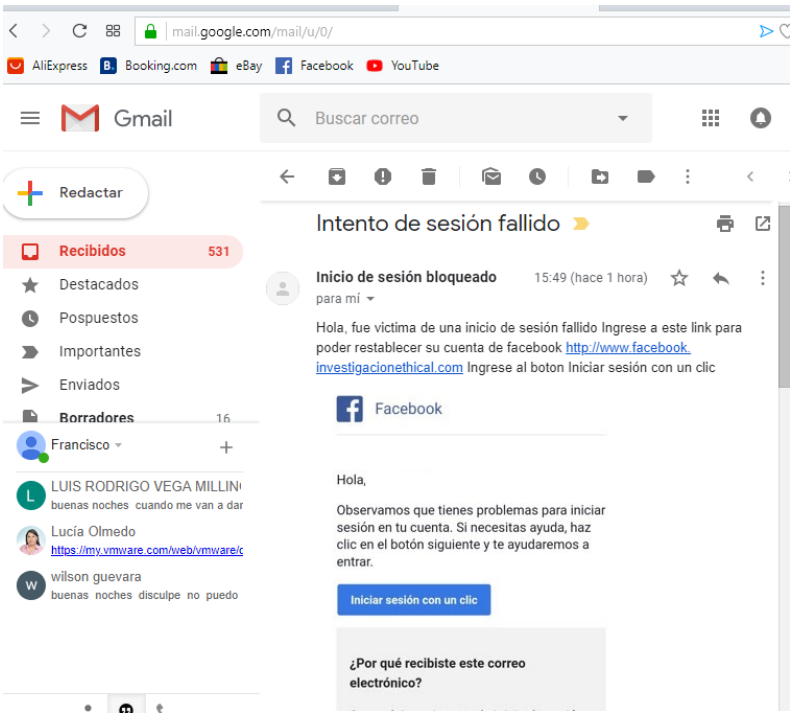

Figura 74 Correo víctima Gmail
Elaborado: Francisco Alvear

Ataque de Mailing

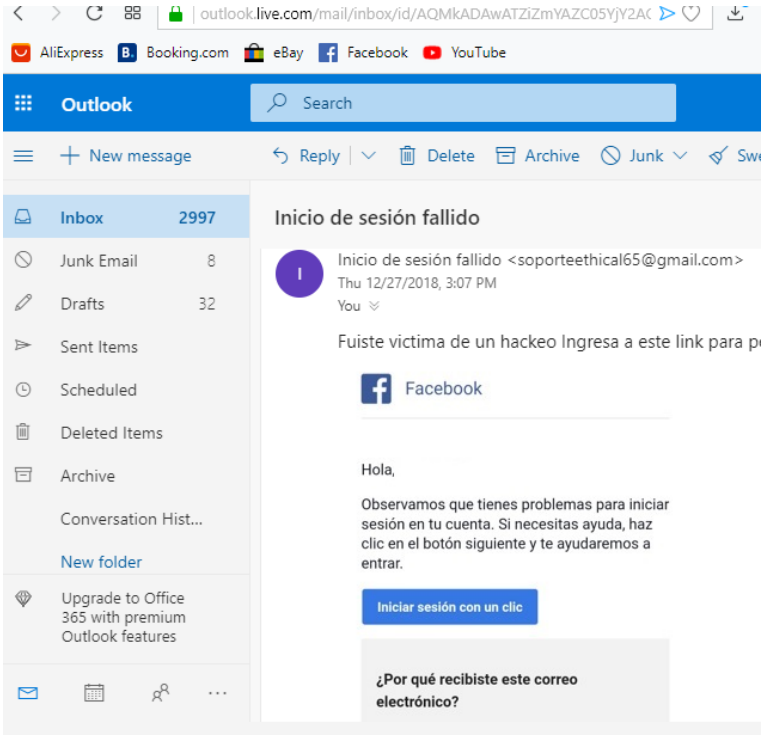

Figura 75 Correo víctima Hotmail
Elaborado: Francisco Alvear

Ataque de Mailing

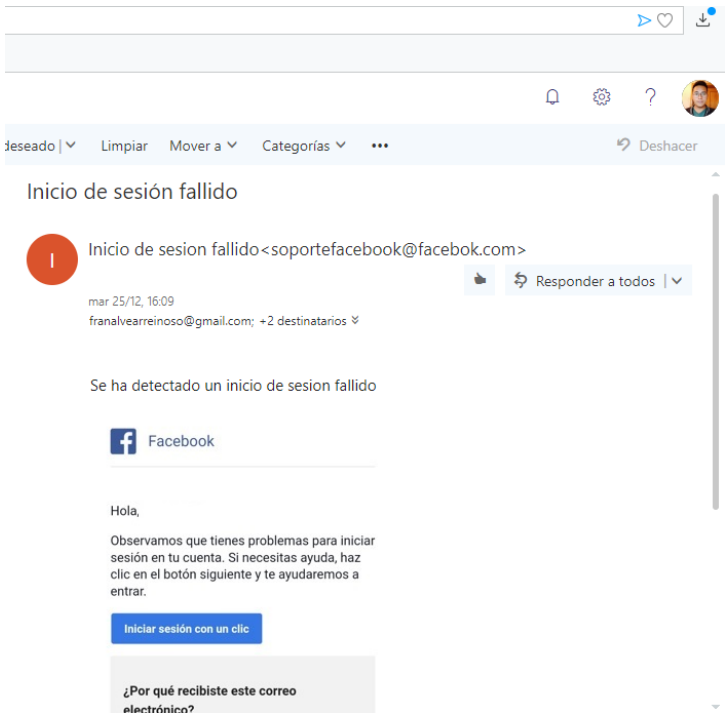

Figura 76 Correo víctima UPS
Elaborado: Francisco Alvear

De esta manera este tipo de ataques agilita el envío de correo electrónicos a un número mayor de potenciales víctimas y así tener un éxito mayor por medio del ataque de *phishing*.

2.1.2.4. Ataque Bomba de correos electrónicos

Para este tipo de ataque se utiliza una herramienta que se encuentra en *GitHub* y se la clona dentro de la instancia virtual. Esta herramienta tiene un funcionamiento en el cual se ingresa un correo electrónico de Gmail antes creado, desde el cual se envía un número deseado de correos a una víctima, haciendo que la bandeja de entrada de este usuario llegue a llenarse en cuestión de minutos y provoque rechazo de correos legítimos entrantes.

Para esto el primer paso es clonar esta herramienta desde *GitHub* con el siguiente comando:

Ataque de bomba de correo

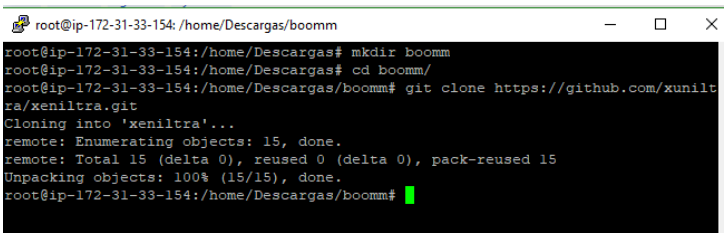

Figura 77 Comando clonación BoomMail
Elaborado: Francisco Alvear

Ya clonada la carpeta con el archivo ejecutable, se corre el archivo con código en Python con el siguiente comando: *./BomMail.py.*

Al ejecutar el archivo se despliega un menú en el cual pregunta qué herramienta de correo se va a utilizar: en este caso se utiliza Gmail. Ingresamos el correo antes creado y la clave, ingresamos el correo de la víctima y un mensaje que va a salir en el correo electrónico y finalmente se coloca cuantos correos son los que van a ser enviados que en este caso fueron 10.

Ataque de bomba de correo

Figura 78 Ataque BomMail
Elaborado: Francisco Alvear

En el correo de la víctima se reflejan los correos enviados

Ataque de bomba de correo

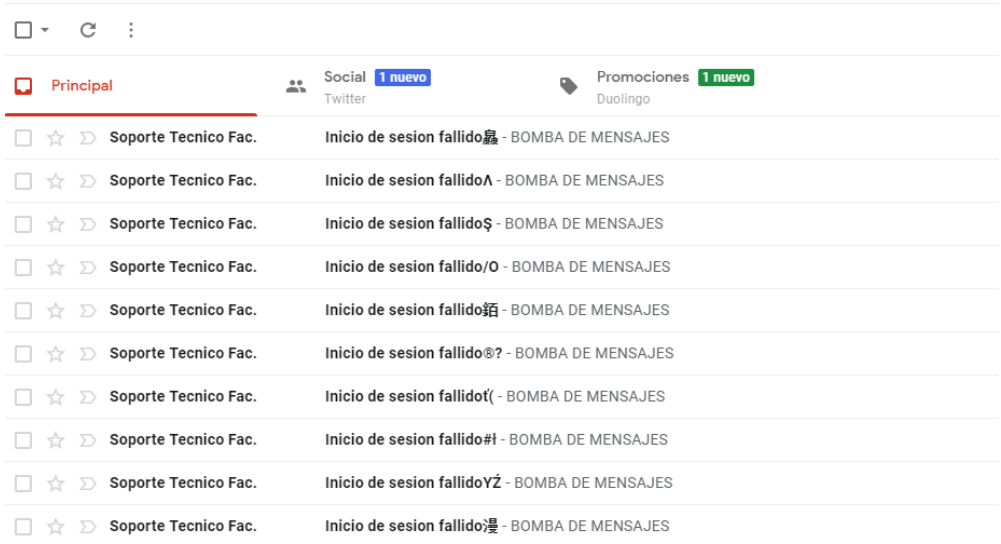

Figura 79 Correo víctima BomMail
Elaborado: Francisco Alvear

De esta manera se puede llegar a saturar un servidor de correo electrónico por medio del envío de un número gigante de correos mediante esta herramienta levantada sobre una instancia virtual.

2.1.2.5. Ataque de Metasploit a usuario.

Metasploit es un conjunto de programas que tienen como objetivo conocer cuáles son las vulnerabilidades de los ordenadores, en este ejemplo se utiliza la herramienta SET levantada en la instancia virtual de Amazon Web Service. El procedimiento del ataque inicia con la ejecución de la herramienta SET.

Ataque de metasploit

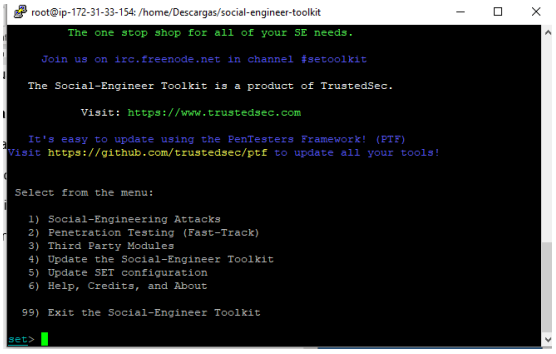

Figura 80 Ejecución herramienta SET
Elaborado: Francisco Alvear

Se elige la primera opción ya que es un ataque de ingeniería social, a continuación, se debe elegir la opción 9 el mismo que es un ataque por Powershell.

Ataque de metasploit

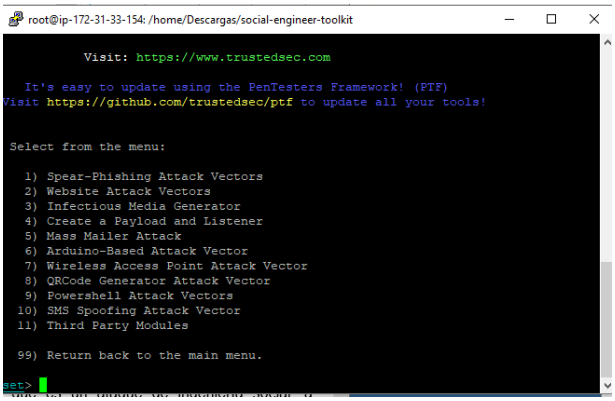

Figura 81 Menú ataque Powershell
Elaborado: Francisco Alvear

En el menú del ataque por Powershell se encuentran diferentes formas de utilizar este ataque, se elige la opción 1 que es una inyección de código shell, el mismo que genera un archivo de texto dentro de la carpeta (cd /root/.set/reports/powershell/).

Ataque de metasploit

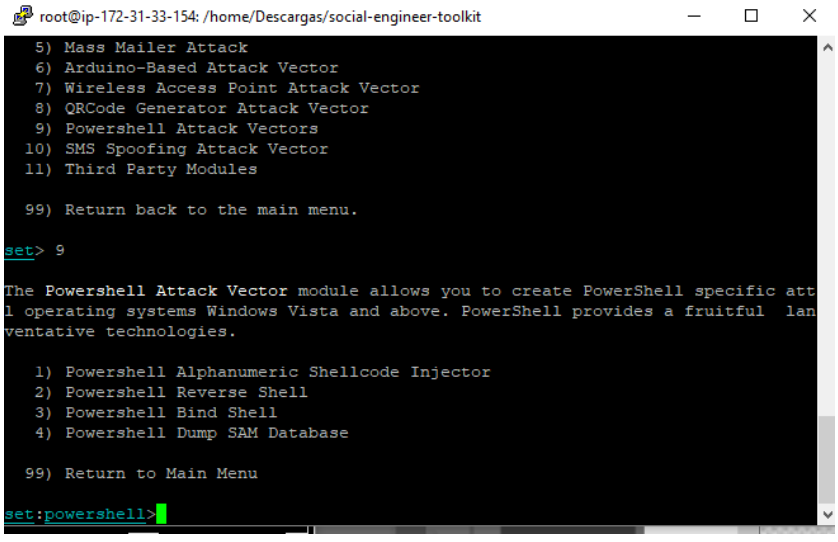

Figura 82 Menú ataque Powershell
Elaborado: Francisco Alvear

Al elegir la opción 1, la herramienta requiere la dirección IP Publica de la instancia virtual la misma que se encuentra en escucha en todo momento a la espera de una

víctima, adicional pide que el puerto 443 este abierto en la máquina virtual para que la comunicación sea efectiva y para finalizar pregunta la herramienta si desea está en escucha la herramienta a lo que se responde con yes.

Ataque de metasploit

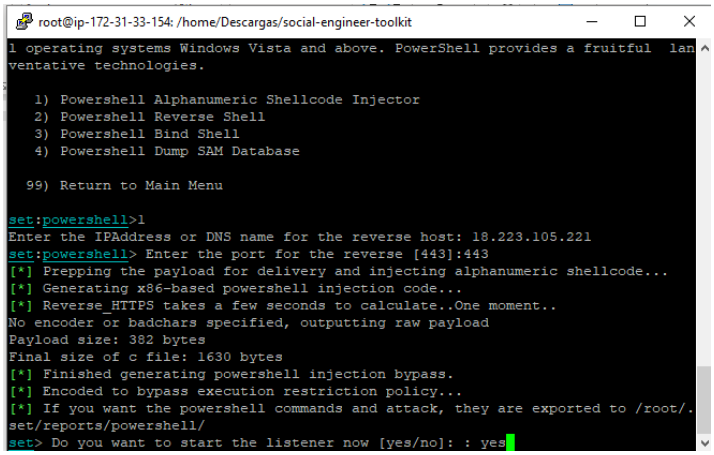

Figura 83 Configuración ataque Powershell
Elaborado: Francisco Alvear

La herramienta se mantiene en escucha hasta que el programa malicioso sea ejecutado en un ordenador, el mensaje que muestra en su pantalla es:

Ataque de metasploit

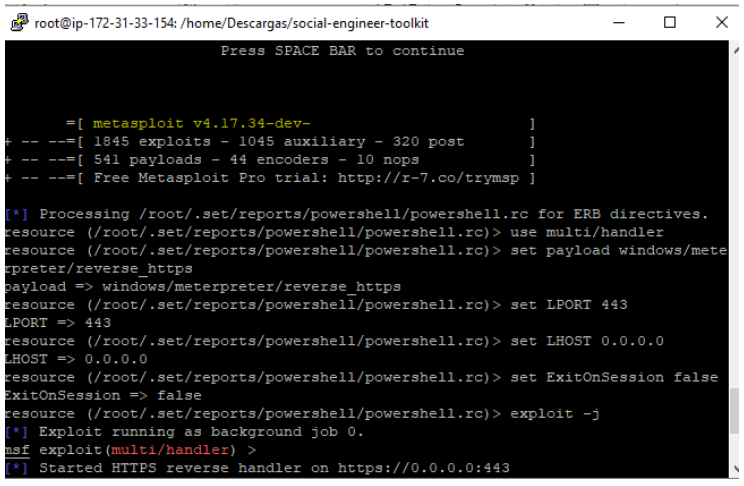

Figura 84 Herramienta SET en escucha
Elaborado: Francisco Alvear

El archivo de la carpeta /root/.set/reports/powershell/ se encuentra con el nombre "x86_powershell_injection.txt" se procede a copiar este archivo con el siguiente comando: cp x86_powershell_injection.txt /home/Descargas/, ya que el archivo se encuentra copiado en Descargas por medio de cualquier herramienta de transferencia de archivos se descarga a un ordenador.

En el ordenador se procede en este caso a cambiar el nombre del archivo a muerte.bat, este archivo por el tipo de extensión es detectable por cualquier tipo de antivirus es por esto que mediante la herramienta Bat To Exe Converter se convierte al archivo .bat a un archivo ejecutable .exe, el nuevo archivo muerte.exe puede llegar a no ser detectado por los antivirus ya que tiene un tipo de extensión igual a los ejecutables de programas legítimos. El archivo ejecutable queda de esta manera

Ataque de metasploit

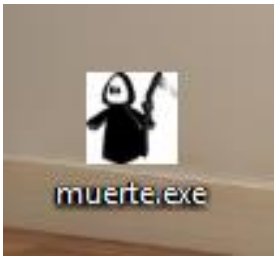

Figura 85 Ejecutable ataque Powershell
Elaborado: Francisco Alvear

Al ejecutar este archivo se presenta lo siguiente en el ordenador infectado.

Ataque de metasploit

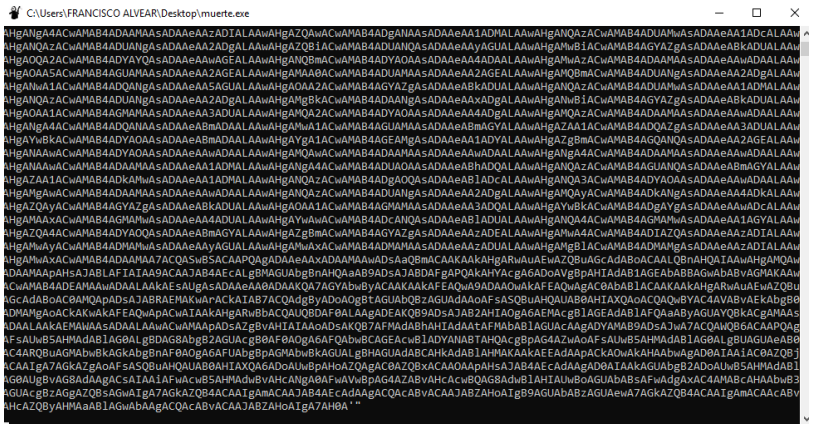

Figura 86 Archivo ejecutado ataque Powershell
Elaborado: Francisco Alvear

En la instancia virtual que se mantiene en escucha se genera el siguiente mensaje alertando al atacante que la víctima ya hizo una conexión con la herramienta y puede tener el control del ordenador.

Ataque de metasploit

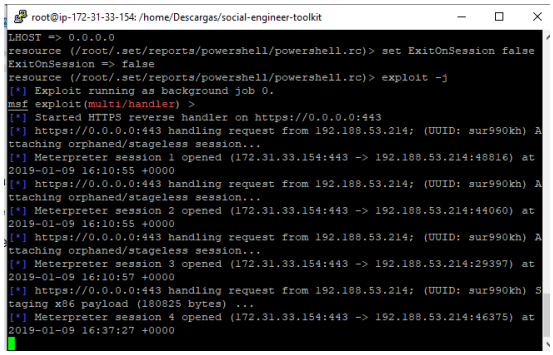

Figura 87 Alerta inicio de sesión en victima ataque Powershell
Elaborado: Francisco Alvear

Se pueden comprobar las sesiones iniciadas con el comando *sessions* en la herramienta.

Ataque de metasploit

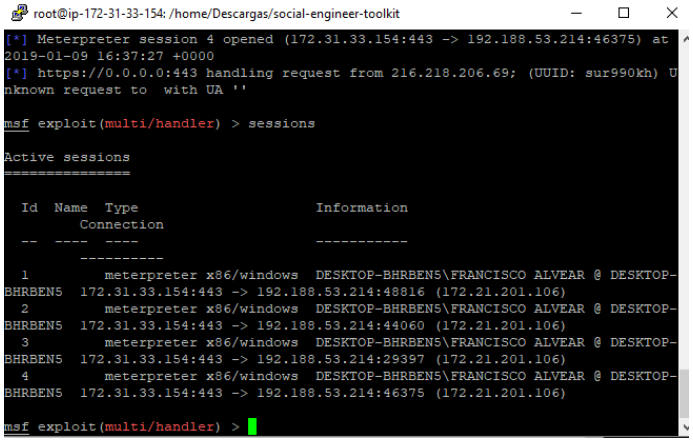

Figura 88 Sesiones iniciadas en ataque Powershell
Elaborado: Francisco Alvear

Para tener iniciar sesión en el ordenador de la víctima se ejecuta el siguiente comando: sesión -i 1.

Se presenta una interfaz de meterpreter con el cual se puede ejecutar comandos para obtener información importante del ordenador de la víctima.

La información que se obtiene mediante el comando *sysinfo* es la siguiente:

Ataque de metasploit

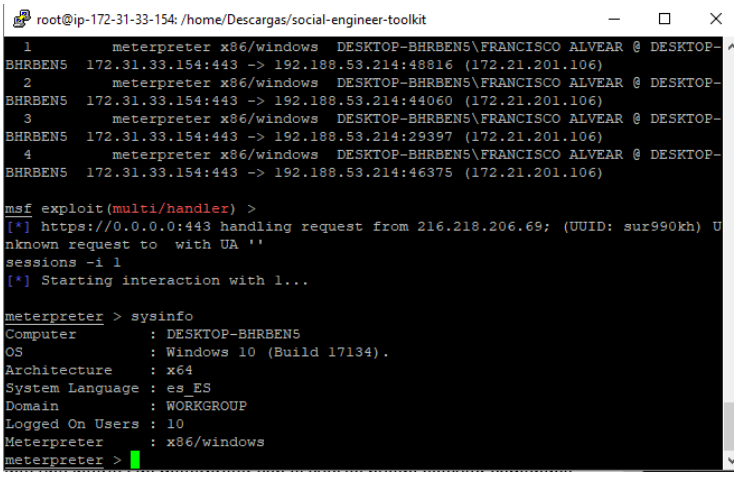

Figura 89 Información comando sysinfo ataque Powershell
Elaborado: Francisco Alvear

La información que busca un atacante es verificar la red interna por la cual se conecta la víctima y esta información se genera con el comando *ipconfig*.

Ataque de metasploit

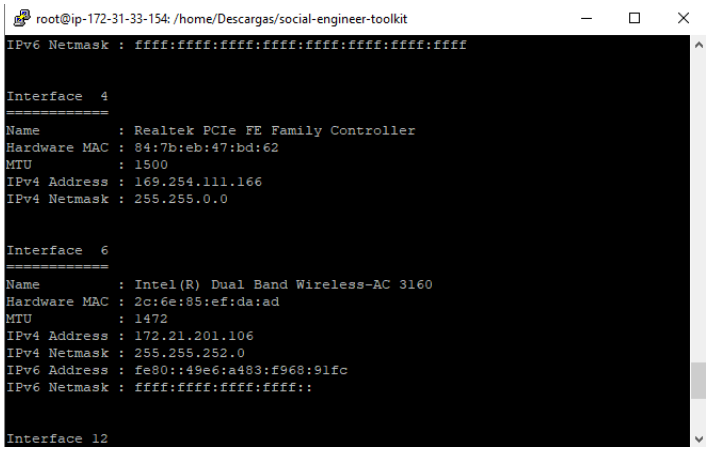

Figura 90 Información de red interna ataque Powershell
Elaborado: Francisco Alvear

Uno de los comandos que más compromete a los ordenadores de las víctimas es: keyscan_start, con este comando iniciamos un sniffer dentro del ordenador de la víctima en donde se guarda todo lo que se vaya escribiendo mientras este en escucha el sniffer, como ejemplo se escribe en un bloc de notas lo siguiente:

Ataque de metasploit

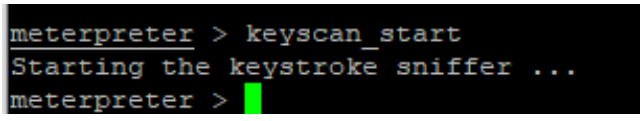

Figura 91 Inicio ataque keyscan
Elaborado: Francisco Alvear

Ataque de metasploit

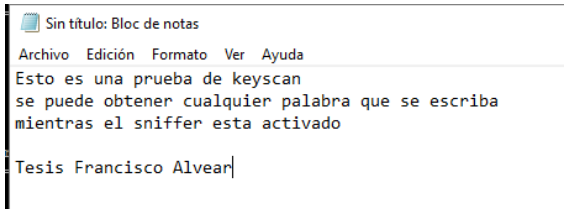

Figura 92 Bloc de notas prueba keyscan
Elaborado: Francisco Alvear

Ya escrito en un bloc de notas se puede comprobar mediante el comando keyscan_dump todo lo que se escribió mientras el sniffer está activado dando como resultado lo siguiente:

Ataque de metasploit

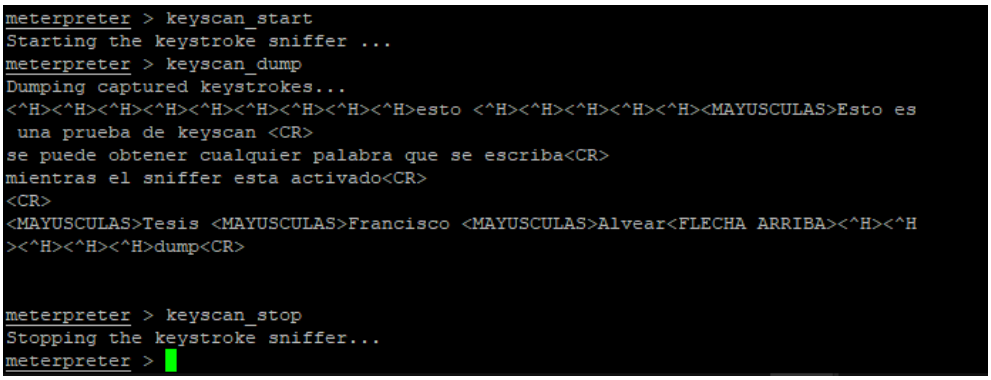

Figura 93 Captura de sniffer ataque keyscan
Elaborado: Francisco Alvear

De esta manera el atacante tiene acceso a información del ordenador de la víctima mientras el programa se ejecuta en segundo plano sin que la persona tenga la idea de que este programa está recopilando información importante sobre la víctima.

CAPITULO 3

ANALISIS E INTERPRETACIÓN DE DATOS

3. Descripción de la población investigada

Para la investigación se obtuvieron 200 correos electrónicos de carácter personal, institucional y empresarial, los mismos que fueron sometidos a cuatro tipo de ataque: *Spoofing*, *Phishing*, *Mailing* y Bomba de Correos.

3.1.1. Tabla de contenidos

Correos Obtenidos

Tabla 3 Correos obtenidos para la investigación

ORD	CORREOS	Nro.	%
1	Correos personales	86	43%
2	Correos institucionales	95	48%
3	Correos empresariales	19	10%
4	Total número de correos	200	100%

Nota: Números de correos por tipo de servidor de correo

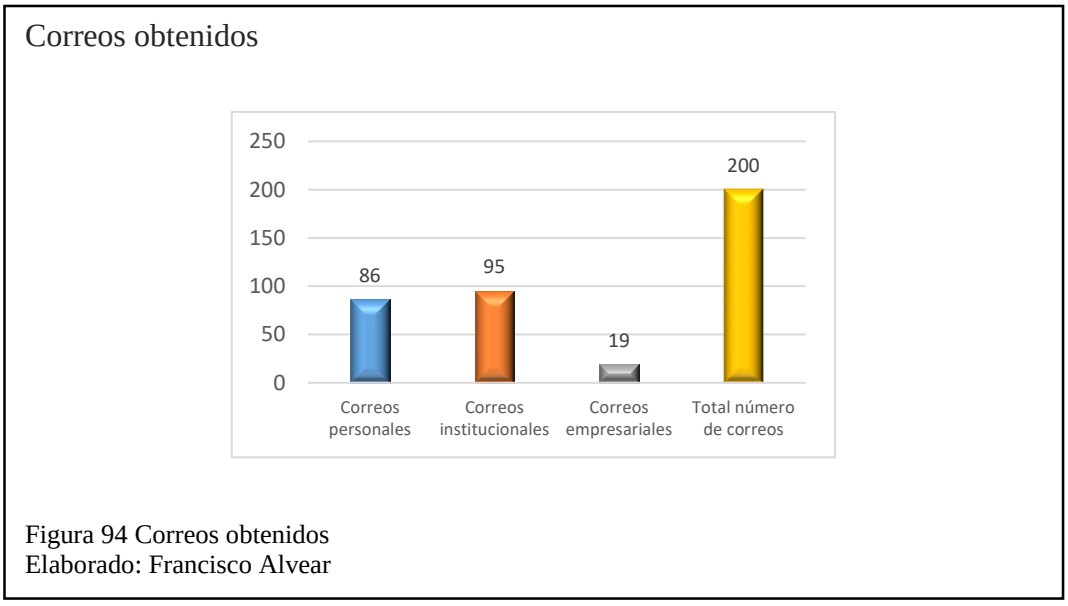

Figura 94 Correos obtenidos
Elaborado: Francisco Alvear

Para la investigación se obtuvieron 200 correos, de los cuales 95 que equivalen al 48% son institucionales; 86 (43%) personales y 19 (10%) empresariales. Todos los correos estuvieron activos y en capacidad para recibir todo tipo de mensajes.

Tipos de correos por estrato

Tabla 4 Tipos de correos por estrato

ORD	TIPOS DE CORREOS	Nro.	%
1	Correos de sexo femenino	64	32%
2	Correos de sexo masculino	136	68%
3	Correos de Nivel Superior	91	46%
4	Correos de Nivel Estudiantes	109	54%
5	Correos de edad entre 21-25	92	46%
6	Correos de edad entre 25-30	67	34%
7	Correos de edad entre 31-35	24	12%
8	Correos de edad entre 36-ADELANTE	17	9%

Nota: Tipos de correo por sexo, nivel de estudio y edad.

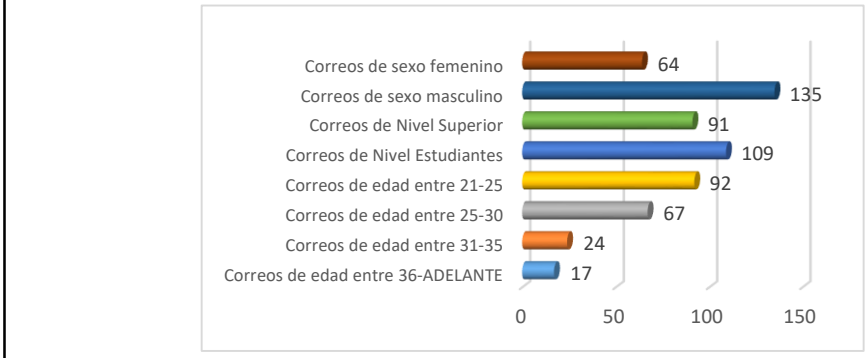

Figura 95 Tipos de correo por estrato
Elaborado: Francisco Alvear

De estos correos, 136 corresponden a hombres, que equivale al 68%, 64 a mujeres (32%); 109 correos son de estudiantes (54%) y 91 de profesionales con título de nivel superior (46%); 92 son de personas entre 21-25 años (46%); 67 de participantes entre 25 y 30 años (34%); 24 de usuarios entre 31 y 35 años (12%) y 17 de personas mayores de 36 años (9%).

Tipos de ataques

Tabla 5 Tipos de ataque

TIPOS DE ATAQUES	CORREOS ENVIADOS	BANDEJA DE ENTRADA	SPAM	BLOQUEADO	TOTAL ENVIADOS
Spoofing	100	80	15	5	95
Phishing	100	70	10	20	80
Mailing con Phishing	200	120	20	60	140
Bomba	50	45	5	0	50
TOTAL ENVIADOS					365

Nota: Correos enviados por tipos de ataques a correos electrónicos

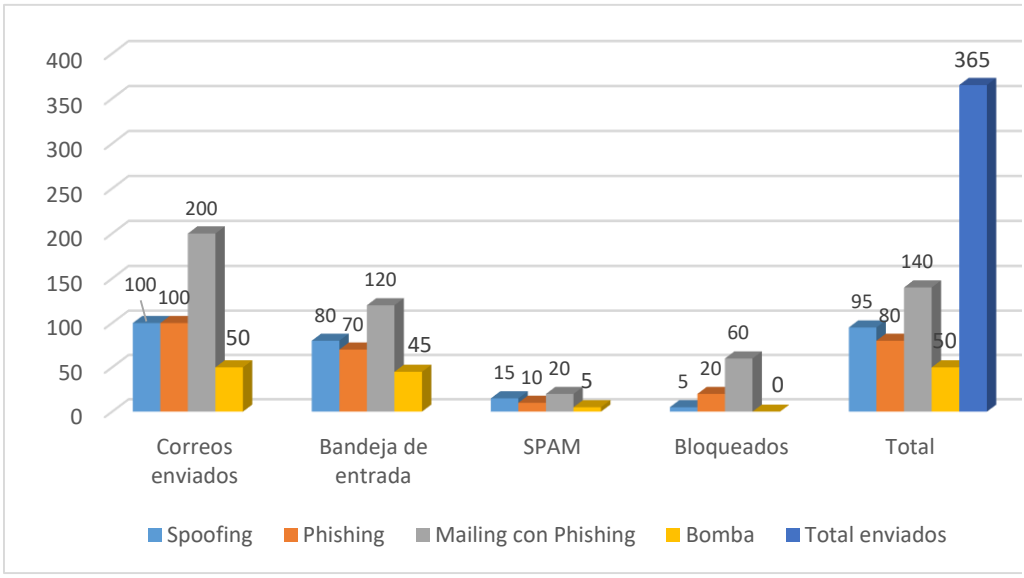

Figura 96 Tipos de correo por estrato
Elaborado: Francisco Alvear

Respecto a los tipos de ataque, se enviaron 100 ataques tipo *Spoofing*, de los cuales 80 ingresaron a la bandeja de entrada; 15 se convirtieron en SPAM y 5 fueron bloqueados, para un total de 95 efectivos.

De 100 ataques tipo *Phishing*, 70 ingresaron a la bandeja de entrada, 10 a SPAM y 20 fueron bloqueados, para un total de 80 efectivos.

Se enviaron 200 ataques de Mailing con *Phishing*, de los cuales 120 ingresaron a la bandeja de entrada, 20 a SPAM, 60 fueron bloqueados para un total de 140 efectivos.

De 50 correos tipo bomba, 45 ingresaron a la bandeja de entrada, 5 a SPAM y ninguno fue bloqueado, para un total de 50 efectivos.

3.2. Resultados de los ataques tipo *Spoofing*

Para la investigación se enviaron 100 ataques tipo *Spoofing*, de los cuales 73 no tuvieron respuesta, 22 abrieron el correo y 5 no se enviaron, como se describe en la siguiente tabla.

Con este tipo de ataque la información que se logró obtener son correos electrónicos y contraseñas para ingresar a la plataforma Facebook, el tipo de suplantación de identidad fue soporte@facebook.com el mismo que genero confianza ante las víctimas y proporcionaron esta información.

3.2.1. Tabla de contenidos

Ataque Spoofing por estracto

Tabla 6 Ataques tipo Spoofing por estracto

SEXO	SIN RESPUESTA	ABRIERON CORREO	NO ENVIADO	TOTAL	%
MASCULINO	50	13	3	66	66%
FEMENINO	23	9	2	34	34%
TOTAL				100	100%

Nota: Datos de ataque Spoofing por sexo

Ataque de spoofing

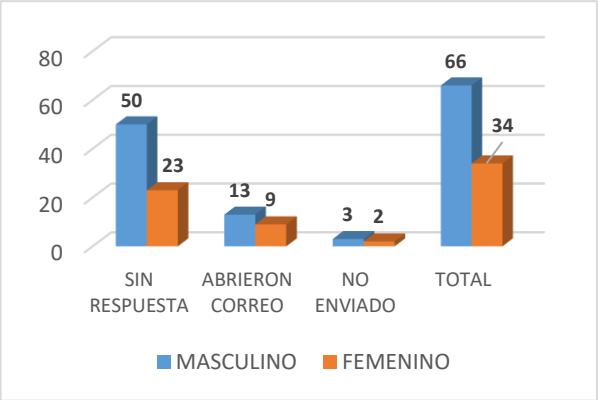

Figura 97 Tipos de correo por estrato
Elaborado: Francisco Alvear

En el ataque tipo Spoofing, 73 no tuvieron respuesta, siendo 50 hombres y 23 mujeres; de 22 que abrieron el correo, 13 son hombres y 9 mujeres y de los no enviados, 3 fueron de correos de usuarios hombres y 2 de mujeres.

Ataque Spoofing por nivel de eduación

Tabla 7 Ataques tipo Spoofing por nivel de educación

EDUCACIÓN	SIN RESPUESTA	ABRIERON CORREO	NO ENVIADO	TOTAL	%
SUPERIOR	28	11	1	40	40%
ESTUDIANTE	45	11	4	60	60%
TOTAL				100	100%

Nota: Datos de ataque Spoofing por nivel de estudio

Ataque de spoofing

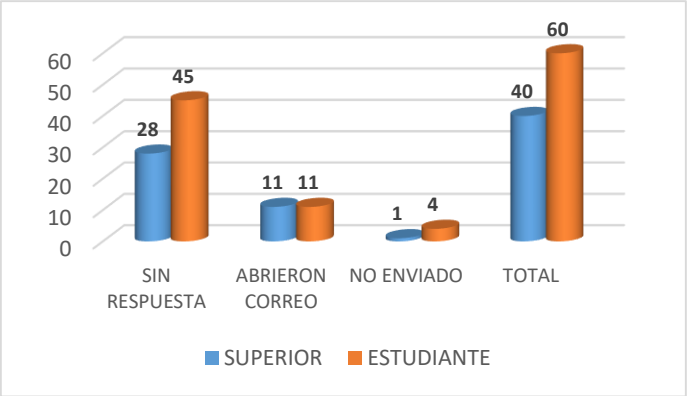

Figura 98 Tipos de correo por nivel educativo
Elaborado: Francisco Alvear

Por el nivel educativo, 28 profesionales con título superior no responden y 45 estudiantes tampoco lo hacen; 11 abrieron el correo en ambos estratos y 1 correo dirigido a un profesional no se envía y no se envían 4 correos dirigidos a estudiantes.

Ataque Spoofing por tipo de correo

Tabla 8 Ataques tipo Spoofing por tipo de correo

TIPO DE CORREO	SIN RESPUESTA	ABRIERON CORREO	NO ENVIADO	TOTAL	%
EMPRESARIAL	15	4	1	20	20%
INSTITUCIONAL	25	6	0	31	31%
PERSONAL	33	12	4	49	49%
TOTAL				100	100%

Nota: Datos de ataque Spoofing por servidor de correo

Ataque de spoofing

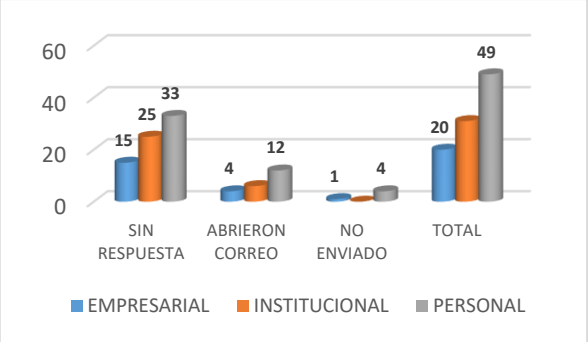

Figura 99 Tipos de correo por tipo de organización
Elaborado: Francisco Alvear

Por el tipo de correo, 15 empresariales, 25 institucionales y 33 personales no tuvieron respuesta; igualmente 4 empresariales, 6 institucionales y 12 personales no abrieron el correo; y, finalmente, 1 correo dirigido a una empresa no se envía y 4 personales, tampoco salen.

Ataque Spoofing por edad

Tabla 9 Ataques tipo Spoofing por edad

EDAD	SIN RESPUESTA	ABRIERON CORREO	NO ENVIADO	TOTAL	%
21-25	30	13	2	45	45%
26-30	21	5	1	27	27%
31-35	9	2	1	12	12%
36-EN ADELANTE	13	2	1	16	16%
TOTAL				100	100%

Ataque de spoofing

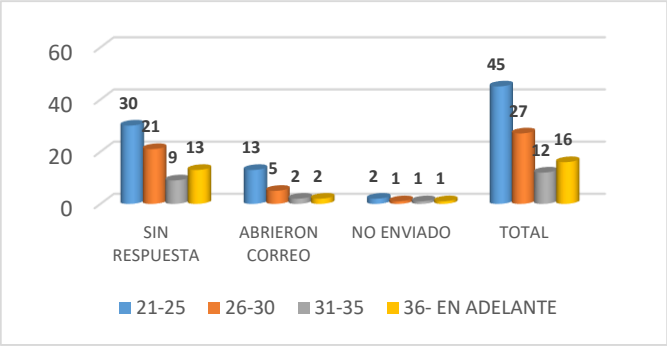

Figura 100 Tipos de correo por edad
Elaborado: Francisco Alvear

Por la edad, 30 correos de usuarios de 21-25 años; 21 de 26-30 años; 9 de 31-35 años y 13 de personas de más de 36 años no tienen respuesta. Igualmente, 13 usuarios de 21-25 años; 5 de 26-30 años; 2 de 31-35 años y 2 de 36 en adelante abrieron el correo; y, 2 correos dirigidos a usuarios de 21-25 años y 1 en los demás estratos no fueron enviados.

3.3. Ataques tipo Phishing

Para valorar la efectividad de los ataques tipo Phishing se enviaron 100 correos, de los cuales 52 no tuvieron respuesta, 28 usuarios abrieron el correo y 20 no fueron enviados.

Por medio de este tipo de ataque se llega a clonar cualquier tipo de página en especial login, en este caso se clono el login de Facebook logrando obtener información de correo y contraseña de las víctimas, en el caso de que el ataque se diera desde un teléfono celular y el login sea automático se llega a obtener correo electrónico o número celular y contraseña de la víctima.

3.4. Tabla de contenidos

Ataque phishing por sexo

Tabla 10 Ataques tipo Phishing por sexo

SEXO	SIN RESPUESTA	ABRIERON CORREO	NO ENVIADO	TOTAL	%
MASCULINO	38	19	16	73	73%
FEMENINO	14	9	4	27	27%
TOTAL				100	100%

Nota: Datos de ataque Phishing por sexo

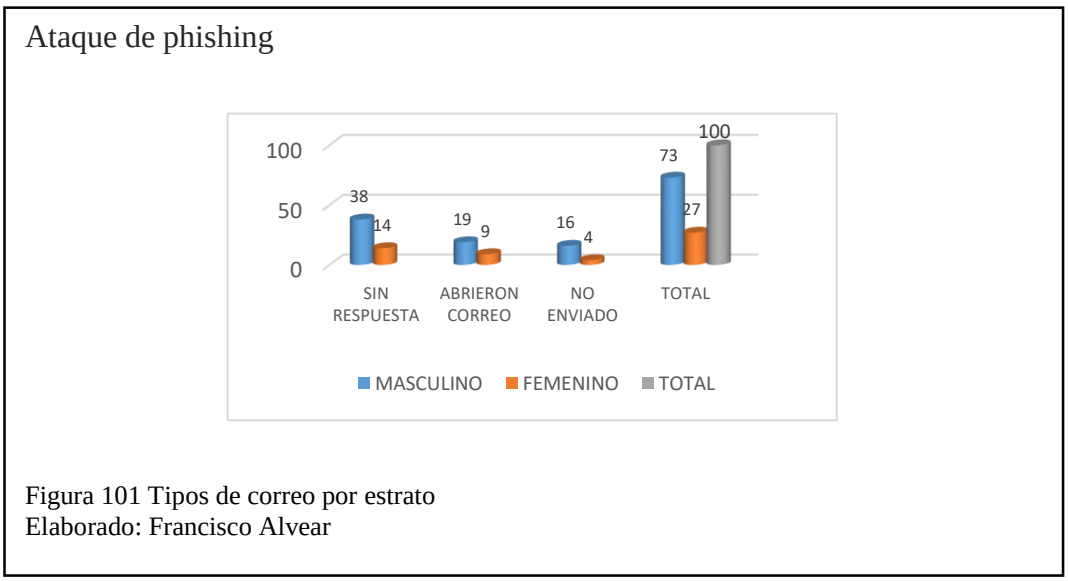

Figura 101 Tipos de correo por estrato
Elaborado: Francisco Alvear

Enviado el ataque tipo Phishing, de 100 correos enviados 38 usuarios hombres y 14 mujeres no emitieron respuesta; 19 hombres y 9 mujeres abrieron los correos y 16 correos no fueron enviados a usuarios hombres y 4 a mujeres.

Ataque phishing por nivel de educación

Tabla 11 Ataques tipo Phishing por nivel de educación

EDUCACIÓN	SIN RESPUESTA	ABRIERON CORREO	NO ENVIADO	TOTAL	%
SUPERIOR	16	7	7	30	30%
ESTUDIANTE	36	21	13	70	70%
TOTAL				**100**	**100%**

Nota: Datos de ataque Phishing por nivel de estudio

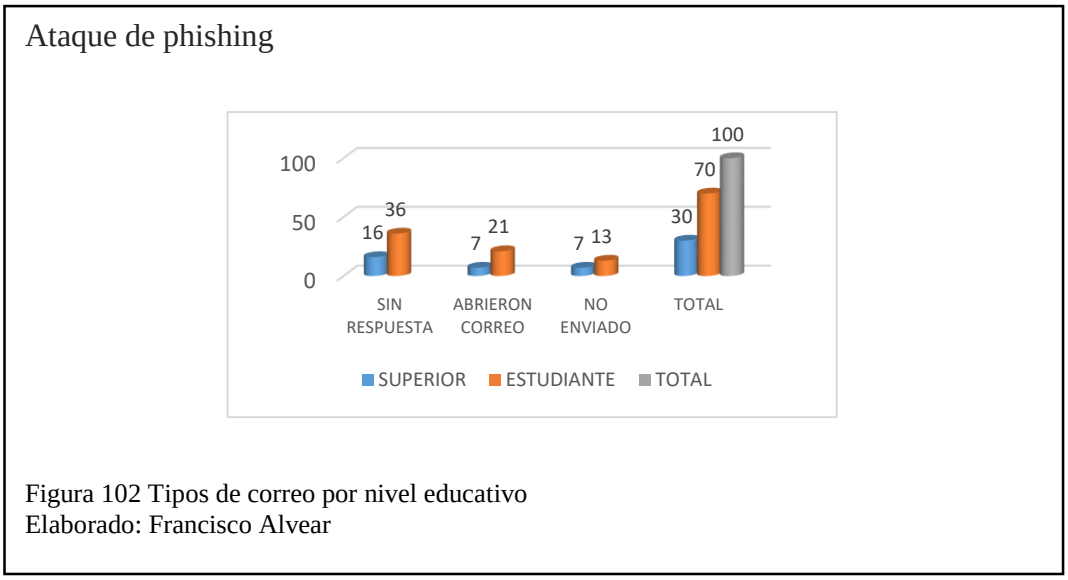

Figura 102 Tipos de correo por nivel educativo
Elaborado: Francisco Alvear

Por el nivel educativo; 16 correos de usuarios de nivel superior y 36 de estudiantes no generaron respuesta; 7 profesionales y 21 estudiantes abrieron los correos y no se enviaron 7 correos a usuarios de nivel superior y 13 a estudiantes.

Ataque phishing por tipo de correo

Tabla 12 Ataques tipo Phishing por tipo de correo

TIPO DE CORREO	SIN RESPUESTA	ABRIERON CORREO	NO ENVIADO	TOTAL	%
EMPRESARIAL	0	0	0	0	0%
INSTITUCIONAL	33	18	13	64	64%
PERSONAL	19	10	7	36	36%
TOTAL				**100**	**100 %**

Nota: Datos de ataque Phishing por servidor de correo

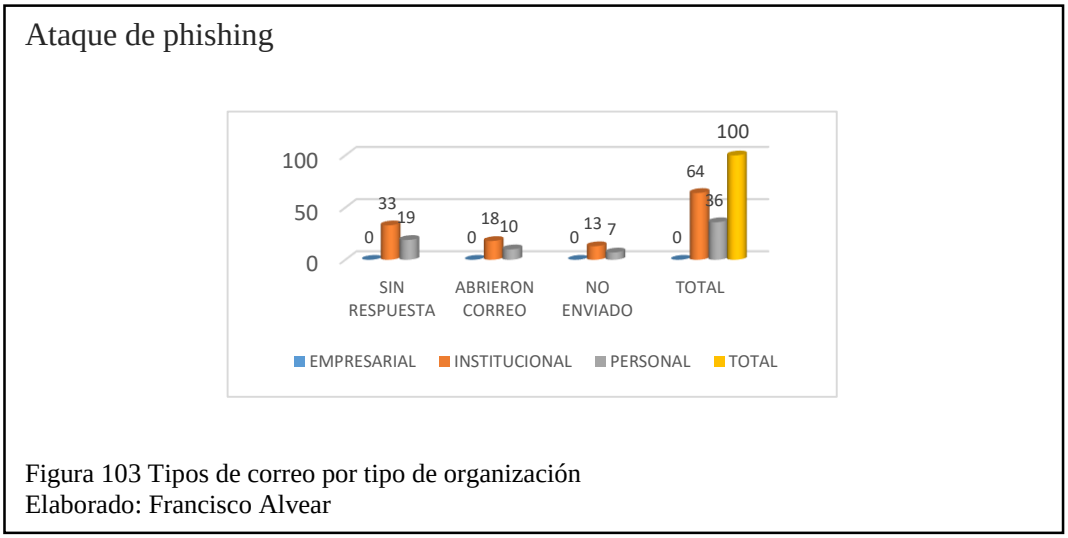

Figura 103 Tipos de correo por tipo de organización
Elaborado: Francisco Alvear

Por tipo de correo, 33 institucionales y 9 personales no tuvieron respuesta; no abrieron los correos 18 institucionales y 10 personales y no se enviaron 13 institucionales y 7 personales.

Ataque phishing por edad

Tabla 13 Ataques tipo Phishing por edad

EDAD	SIN RESPUESTA	ABRIERON CORREO	NO ENVIADO	TOTAL	%
21-25	26	14	7	47	47%
26-30	19	11	10	40	40%
31-35	7	2	3	12	12%
36- EN ADELANTE	0	1	0	1	1%
TOTAL				**100**	**100%**

Nota: Datos de ataque Phishing por edad

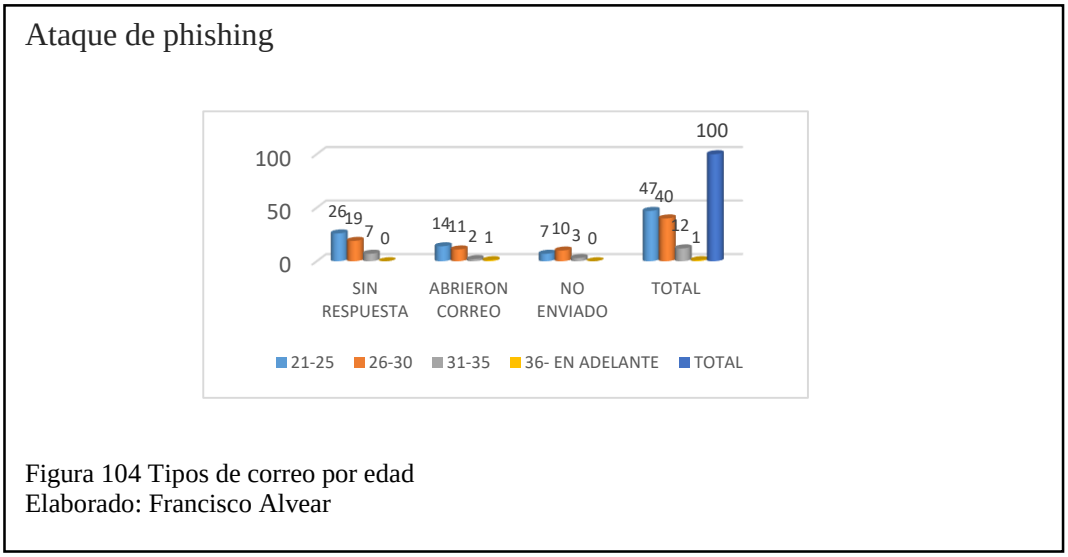

Figura 104 Tipos de correo por edad
Elaborado: Francisco Alvear

Por la edad, no tuvieron respuesta 26 correos, en rangos de 21-25; 19, en rango de 26-30 años y 7, en intervalo 31-35 años. Abrieron sus correos 14 usuarios en rango de edad 21-25 años; 11, entre 26-30 años; 2, de 31-35 años y 1, de 36 en adelante. No se enviaron 7 correos a usuarios de 21-25 años; 10 de 26-30 años, y 3 de 31-35 años.

3.5. Ataques tipo Mailing

Para obtener resultados de investigación se enviaron 200 correos con ataques tipo mailing, de los cuales 105 no tuvieron respuesta, 35 usuarios abrieron sus correos y 60 no se enviaron, como se evidencia en los datos que se exponen a continuación:

3.5.1. Tabla de contenidos

Ataque mailing por sexo

Tabla 14 Ataques tipo Mailing por sexo

SEXO	SIN RESPUESTA	ABRIERON CORREO	NO ENVIADO	TOTAL	%
MASCULINO	74	24	41	139	70%
FEMENINO	31	11	19	61	31%
TOTAL				200	100%

Nota: Datos de ataque Mailing por sexo

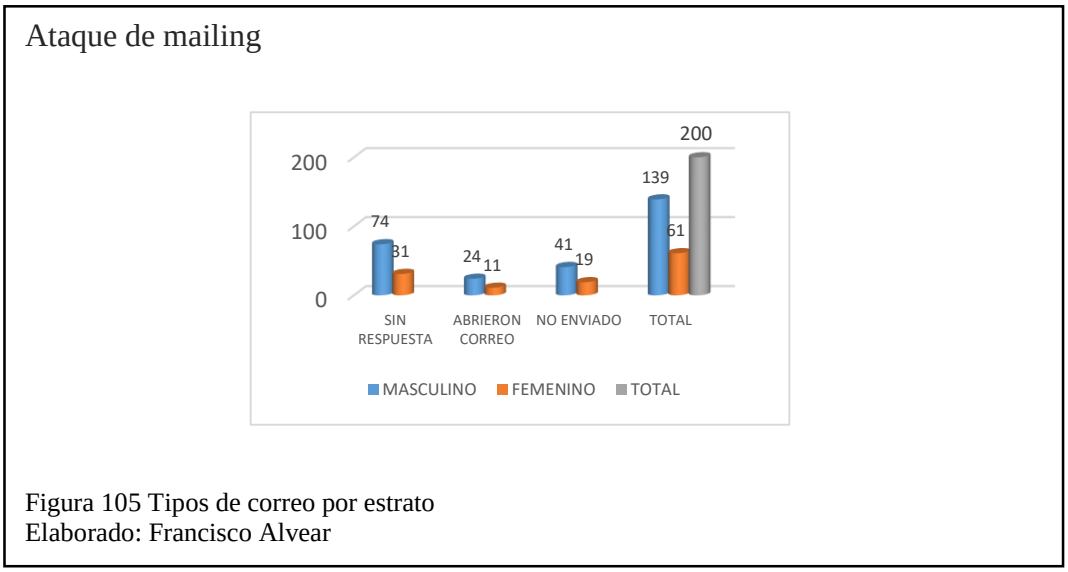

Figura 105 Tipos de correo por estrato
Elaborado: Francisco Alvear

De 200 ataques tipo Mailing, no tuvieron respuesta 74 de usuarios hombres y 31 de mujeres; 24 hombres abrieron su correo y no lo hicieron 11 mujeres; 41 correos no se enviaron a hombres y 19 a mujeres.

Ataque mailing por nivel de educación

Tabla 15 Ataques tipo Mailing por nivel de educacion

EDUCACIÓN	SIN RESPUESTA	ABRIERON CORREO	NO ENVIADO	TOTAL	%
SUPERIOR	47	21	22	90	45%
ESTUDIANTE	58	14	38	110	55%
TOTAL				**200**	**100%**

Nota: Datos de ataque Phishing por nivel de estudios

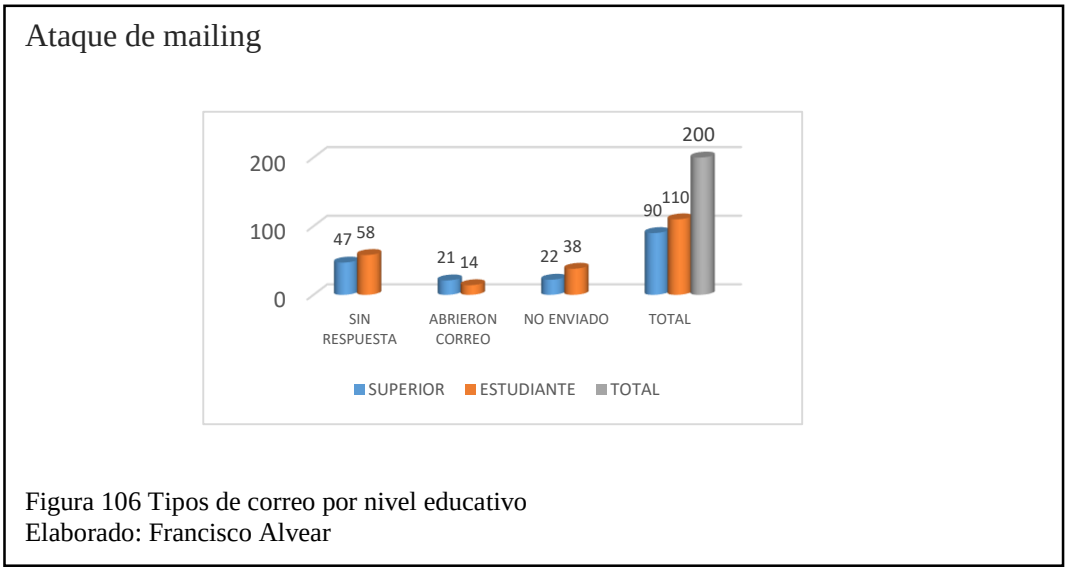

Figura 106 Tipos de correo por nivel educativo
Elaborado: Francisco Alvear

Por el nivel educativo 47 correos de profesionales y 58 de estudiantes no tuvieron respuesta; 21 usuarios de nivel superior y 14 estudiantes abrieron sus correos y no se enviaron 22 a profesionales y 38 a estudiantes.

Ataque mailing por tipo de correo

Tabla 16 Ataques tipo Mailing por tipo de correo

TIPO DE CORREO	SIN RESPUESTA	ABRIERON CORREO	NO ENVIADO	TOTAL	%
EMPRESARIAL	9	5	5	19	10%
INSTITUCIONAL	51	10	34	95	48%
PERSONAL	45	20	21	86	43%
TOTAL				**200**	**100 %**

Nota: Datos de ataque mailing por servidor de correo

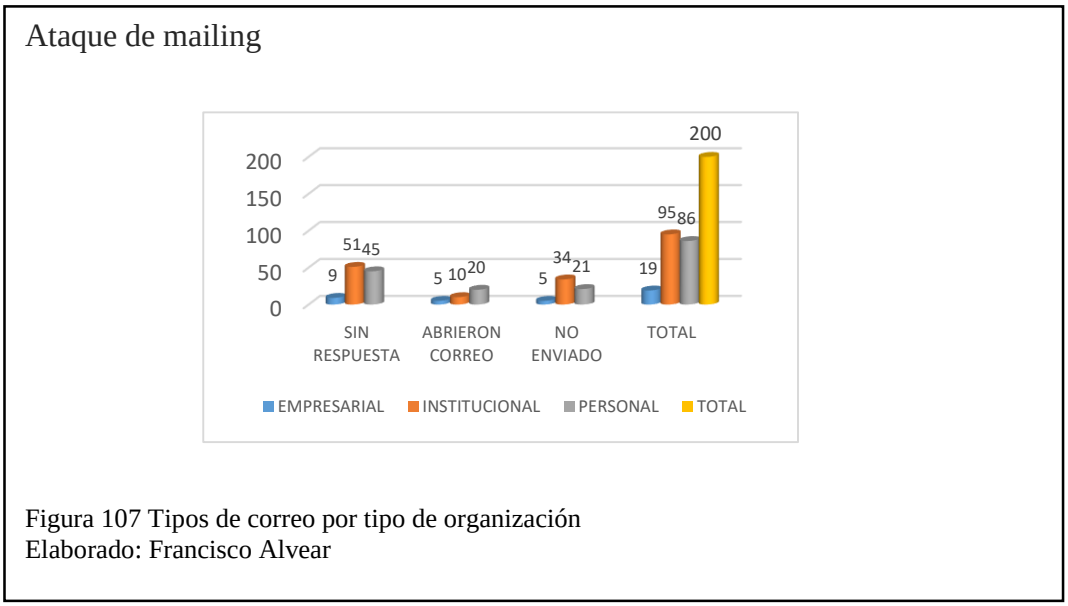

Figura 107 Tipos de correo por tipo de organización
Elaborado: Francisco Alvear

Por tipo de organización, no tuvieron respuesta 9 correos empresariales, 51 institucionales y 45 personales; abrieron su correo 5 usuarios empresariales, 10 institucionales y 20 personales. No se enviaron 5 correos a empresas, 34 a instituciones y 21 a personas naturales.

Ataque mailing por edad

Tabla 17 Ataques tipo Mailing por edad

EDAD	SIN RESPUESTA	ABRIERON CORREO	NO ENVIADO	TOTAL	%
21-25	53	18	21	92	46%
26-30	31	8	28	67	34%
31-35	11	6	7	24	12%
36- EN ADELANTE	10	3	4	17	9%
TOTAL				**200**	**100%**

Nota: Datos de ataque mailing por edad

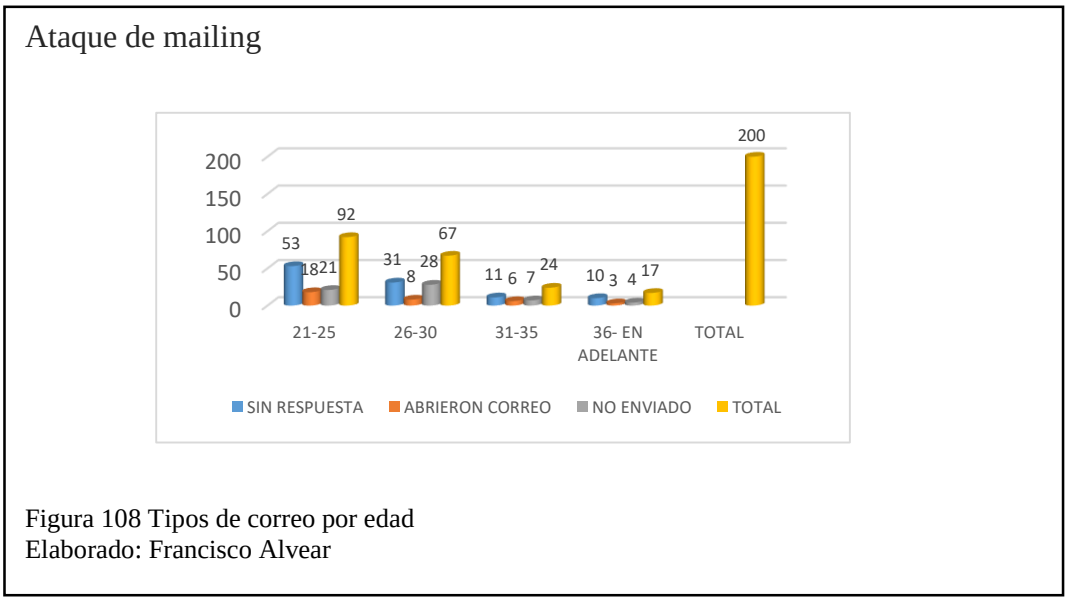

Figura 108 Tipos de correo por edad
Elaborado: Francisco Alvear

No tuvieron respuesta 53 correos de usuarios entre 21-25 años, 31, de 26-30 años, 11, de 31-35 años y 10, de 36 en adelante. Abrieron su correo 18 usuarios de 21-25 años; 8, de 26-30 años; 6, de 31-35 años y 3, de más de 36 años. No se enviaron 21 correos a usuarios de 21-25 años; 28, a personas de 26-30 años; 7, de 31-35 años y 4, de más de 36 años.

3.6. Ataques tipo Bomba

3.6.1. Tabla de contenidos

Tabla 18 Ataques tipo Bomba y resultados obtenidos

ORD.	ESTATUS	Nro.	%
1	SIN RESPUESTA	0	0%
2	ABRIERON CORREO	50	100%
3	NO ENVIADOS	0	0%
TOTAL		50	100%

Nota: Datos de ataque bomba

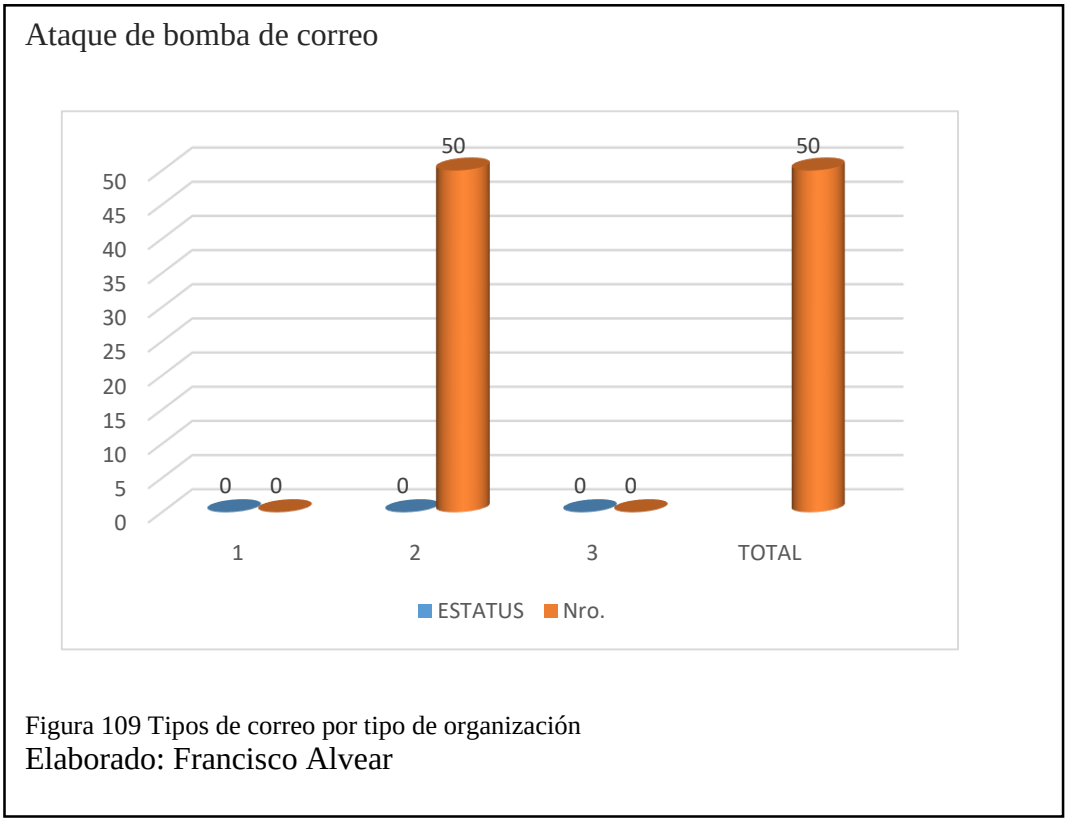

Figura 109 Tipos de correo por tipo de organización
Elaborado: Francisco Alvear

Para análisis el impacto en los usuarios, se enviaron 50 correos con una efectividad del 100% pues todos los usuarios abrieron sus correos, generando saturación inmediata en la bandeja de entrada.

3.7. Propuesta de solución Spoofing.

3.7.1. Soluciones Técnicas

3.7.1.1. Solución por Software

Desde el punto de vista la solución para evitar los ataques de tipo MailSpoofing es la detección de la vulnerabilidad en el servidor de correo electrónico, la verificación del servidor DNS con el comando nslookup -type = txt midominio.com, se puede verificar la cabecera SPF instalada en DNS desde donde se envía el correo electrónico.

Soluciones ataques de correo electrónico

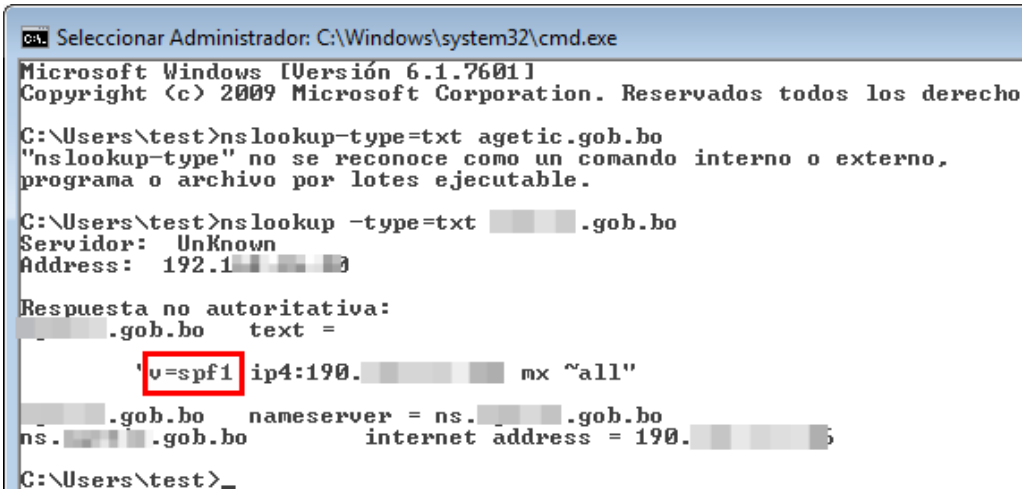

Figura 110 Verificación cabecera SPF
Fuente: (ÁLVAREZ, 2017)

Se debe verificar las cabeceras de los correos electrónicos recibidos.

Soluciones ataques de correo electrónico

Figura 111 Verificación cabeceras de correo electronico
Fuente: (ÁLVAREZ, 2017)

Como se puede observar en la figura 108 las cabeceras SPF se encuentran presentes, como medida se recomienda utilizar sistemas que encripten él envió y comunicación por correo entre servidores y la utilización de programas de autenticación mediante las cabeceras de correo electrónico.

Los métodos de autenticación de correos electrónicos son:

- SPF: Sender Policy Framework, este sistema de verificación de correo compara el dominio del cual fue enviado y la dirección IP pública de origen con las Ips autorizadas para la recepción de correos legítimos.
- SenderID: Verifica las cabeceras SPF y mejora las medidas de seguridad considerando también las cabeceras RFC 4407
- DKIM: DomainKEys Identified Mail este método permite utilizar una firma digital o certificado que garantiza que el correo no fue modificado desde el envío hasta la recepción en el servidor de correo entrante. (informáticos, 2017)

3.7.2. Solución por medio de capacitación

Si bien existen muchos métodos y programas para poder defender el servidor de correo electrónico de ataques, estos no son 100% eficientes mientras los usuarios finales no se encuentren capacitados para no ser víctimas de este tipo de ataque es por esto por lo que se recomienda capacitaciones regulares y dar a conocer aspectos mínimos de seguridad como los siguientes:

- Evitar el registro en sitios Web con correos electrónicos empresariales ya que de obtienen una puerta por donde ingresar con un ataque.
- Evitar el acceso de enlaces directamente desde el correo electrónico, verificar en un navegador si este enlace es seguro para poder ingresar
- No descargar ningún archivo adjunto a correos electrónicos que se tenga sospecha que es falso aun si el remitente es una persona conocida o del mismo dominio.
- Si un usuario de la empresa abrió un correo malicioso y brindo información importante de esta, aislar el equipo y asegurar la información provista.
- Verificar las cabeceras de los correos recibidos y que se sospecha sean un ataque de suplantación de identidad.
- Notificar a personas conocidas de este tipo de ataques para evitar la propagación de este.

3.8. Propuesta de solución Phishing.

3.8.1. Soluciones Técnicas

3.8.1.1. Solución por Software

Para poder dar tratamiento a los correos con phishing es importante verificar los servidores de correo del cual fueron enviados.

Todos los mensajes de correo electrónico incluyen información del servidor de donde salieron, la información que contienes es: IP desde donde se envía el correo, el programa que se utiliza para la redacción del correo y los servidores por donde viaja el mensaje hasta llegar a la víctima.

Existen filtros que verifican que esta información sea verdadera y de esta forma identifican problemas con la autenticación del servidor de donde fue enviado el correo electrónico.

Los atacantes utilizan hosting gratuitos para enviar los correos con el enlace a página web falso, utilizando varios ataques unidos hacen que a las personas que llegan este correo lo vea como un mensaje verídico y caiga en la trampa.

Los servidores de correo electrónico que más se utiliza para el reenvió de correos con phishing son:

- Thunderbird/Icedove
- Webmail SquirrelMail
- The Bat
- Outlook Express

3.8.2. Solución por medio de capacitación

La capacitación en este tipo de ataque es muy importante ya que en un mayor porcentaje es efectivo por la desinformación del usuario final y es esta vulnerabilidad la que el atacante aprovecha para poder robar información personal o financiera de la víctima

Para esto se tienen las siguientes soluciones para evitar ser atacado por medio de correo electrónico:

- Evitar los correos SPAM ya que por este medio se distribuyen los mensaje engañosos, toda acción que contribuya a eliminar o bloquear correos SPAM reducirá los mensajes de phishing y de esta manera evita el ataque.
- En ningún caso las empresas o bancos solicitan datos personales o financieros por medio del correo electrónico, llamadas telefónicas ni fax. Los bancos nunca envían correos a sus usuarios para la actualización de datos mediante un enlace a la página web, es importante no ingresar usuario y clave en páginas web de dudosa procedencia, siempre es importante verificar el certificado SSL.
- Es importante no contestar a los correos que piden información personal o financiera y verificar con el banco por medio de una llamada telefónica a los números oficiales y no con los que se ponen en el correo electrónico.
- Como medida de seguridad se recomienda escribir el enlace en el navegador web ya que se evita que sea una trampa el enlace escrito en el correo y se re direccione a una página falsa, si el sitio solicita información personal o financiera verificar el envío y recepción de datos por un canal seguro SSL, el enlace debe empezar con https:// y está marcado de color verde lo que significa que es seguro.

3.9. Propuesta de solución Spam

3.9.1. Soluciones Técnicas

3.9.1.1. Solución por Software

El problema principal del SPAM no es que llena la bandeja de entrada del correo electrónico, sino que por este medio llegan todos los ataques de una manera efectiva.

Es por esto que se lo cataloga como un problema a los servidores de correo electrónico y los especialistas en seguridad afirman que bloqueado los correos SPAM se está logrando un avance significativo en seguridad por medio del correo electrónico.

En general la mayor parte de los correos electrónicos SPAM son de mensajes publicitarios que aparte de ser molestos para el usuario logran ocasionar inconvenientes en el funcionamiento normal del servidor de correo haciendo que las

aplicaciones sean lentas y que la bandeja de entrada del servidor de correo se llene y evite que se pueda enviar y recibir correos.

- Es importante no reenviar correos electrónicos que se han recibido como una cadena de mensajes así se evita la propagación del SPAM.
- Si existe la necesidad de enviar un correo a varias personas se recomienda la utilización de la opción CCO para evitar que sea visible los correos a los que están copiados.
- Cuando se revise los correos SPAM es importante no responder ya que de esta manera se sabe cuál de los correos están activos y se puede enviar más publicidad o ataques.
- La utilización de un programa de opción de bloqueo de palabras es importante para que sean bloqueados los correos SPAM, es importante la actualización del sistema operativo, actualización del antivirus y siempre estar activo el firewall.
- No ingresar el correo personal en formularios para evitar el envió de publicidad o filtración en páginas para la utilización de estos correos para ataques cibernéticos.

3.9.2. Solución por medio de capacitación

La capacitación de las personas es un punto muy importante ya que de esta manera evitamos la propagación de este tipo de ataques, es por esto que es necesario tomar en cuenta los siguientes puntos:

- No utilizar correos personales: No publicar el correo electrónico personal en formularios, foros, redes sociales o en internet. Es recomendable utilizar un correo electrónico diferente para el registro en páginas o programas que necesite el usuario
- Al final de un correo que contiene SPAM existe la opción de salir de la lista para que no llegue más correos electrónicos, lo que realmente hace esta acción es verificar que el correo electrónico al que fue enviado la publicidad o ataque está activo.

- Los atacantes buscan bases de datos llenos de correos electrónicos en el internet y prueban enviando a todos los correos electrónicos el ataque hasta que alguna persona caiga en la trampa.
- Usar un filtro SPAM, el software en desarrollo ahora pueden mantener un nivel de administrable de los correos que llegan a la bandeja de entrada, verificando el contenido del correo o el asunto del mismo. Teniendo así una base de datos de palabras que son utilizadas como asunto en un correo con SPAM y haciendo que sea más efectivo la detección de este tipo de correos.

CONCLUSIONES

- La utilización de la instancia virtual de Amazon Web Service hace que los ataques tengan mayor eficacia, ya que, los equipos de seguridad no los pueden detectar debido a que vienen de una fuente confiable.
- SET es una herramienta poderosa para detectar vulnerabilidades y en este caso fue utilizada para poder realizar ataques por medio de correos electrónicos con una eficiencia mayor a herramientas gratuitas.
- El ataque de phishing junto al ataque por ingeniería social llega a tener un fuerte impacto ante las victimas que entregan información tanto personal como financiera.
- Para que un correo electrónico llegue a la bandeja de entrada de los servidores reconocidos necesita pasar por filtros de SPAM y hay que informar a estos filtros que el servidor de correo levantado es real y corresponde a un dominio.
- Las empresas con servidores de correos en Linux son más vulnerables a caer en este tipo de ataque ya que llegan todos los correos enviados, mientras que servidores de correo como Exchange luego de un número considerable de correos enviados desde un mismo dominio los envía directamente a SPAM o los bloquea.
- La mayoría de los correos que se activaron al ser abiertos corresponde a hombres, siendo los usuarios mayoritarios estudiantes en edades comprendidas entre 21-25 años; y también por profesionales con estudios superiores, dependiendo del tipo de ataque.

RECOMENDACIONES

- Se recomienda las empresas mantengan siempre actualizado los servidores de correos electrónicos para así evitar que exista una puerta trasera la cual puedan utilizar para poder realizar ataques.
- Todos los usuarios deben mantener actualizado y activo el antivirus para evitar la ejecución de malwares enviados por correo electrónico y así robar información importante de las víctimas o empresa.
- Se recomienda realizar pruebas de phishing a los usuarios de servidor de correo de una empresa y así saber si necesitan capacitación sobre seguridad de la información.
- Se recomienda utilizar programas donde se pueda abrir correo electrónico como Microsoft Outlook ya que tienen mayor seguridad ante ataques y evitar abrir el servidor de correo en navegadores web.
- El administrador de seguridad de la información debe capacitar periódicamente al personal de la empresa sobre lo tipos de ataques a correos electrónicos y la información tanto personal como empresarial a la que pueden tener acceso y lo que los atacantes pueden hacer con ella.
- Considerar como vulnerables a usuarios hombres comprendidos en el rango de edad de 21-25 años quienes tienen un acceso y manejo extraordinario de paquetes informáticos, internet y correo electrónico, por lo que accidentalmente o de manera intencionada activan ataques a los sistemas o redes de la organización.

LISTA DE REFERENCIAS

Academy, C. N. (01 de 05 de 2018). *Cisco Networking Academy* . Obtenido de https://www.netacad.com/es/courses/security/introduction-cybersecurity

Acens. (05 de 01 de 2015). *acens.* Obtenido de https://www.acens.com/wp-content/images/2017/12/spoofing-wp-acens.pdf

AENOR. (2012). *Sistemas de gestión de seguridad: Protección física de activos.* Madrid: ASIS INTERNATIONAL.

AGUDO, S. (16 de 03 de 2017). *Genbeta.* Obtenido de https://www.genbeta.com/seguridad/el-fbi-explica-como-fue-hackeado-yahoo-mediante-un-ataque-de-spear-phishing

Alvarez, A. A. (s.f.). *Servicio semanal de vigilancia tecnológica o monitoreo temático del entorno sobre Nuevas*. Obtenido de http://www.bc.gob.cu/anteriores/Iconos/2015/Iconos525.pdf

ÁLVAREZ, R. (05 de 05 de 2017). *Xataka.* Obtenido de https://www.xataka.com/seguridad/el-sofisticado-ataque-masivo-de-phishing-que-se-propago-como-polvora-en-gmail-y-google-docs

ASIS INTERNATIONAL. (18 de 01 de 2012). *Sistemas de Gestión de la Seguridad: protección física de los activos.* Madrid: AENOR EDICIONES. Obtenido de https://listas.20minutos.es/lista/11-virus-y-gusanos-informaticos-que-aterrorizaron-al-mundo-1era-entrega-270704/

Basics, C. (27 de 03 de 2013). *Confirma Sistemas.* Obtenido de https://www.confirmasistemas.es/es/contenidos/canal-basics/que-es-el-spoofing

ciyi, C. G. (26 de 08 de 2010). *Hacking Etico.* Obtenido de https://hacking-etico.com/2010/08/26/hablemos-de-spoofing/

Collado, C. (21 de 04 de 2017). *Aplicaciones Android* . Obtenido de https://andro4all.com/2017/04/malware-google-play

CYBERPEDIA. (15 de 10 de 2017). *Paloalto.* Obtenido de https://www.paloaltonetworks.com/cyberpedia/what-is-a-port-scan

Defense, P. A. (09 de 07 de 2018). *Panda.* Obtenido de https://www.pandasecurity.com/spain/mediacenter/seguridad/ataque-empresas-correo-electronico/

Donohue, B. (21 de 10 de 2013). *Kaspersky Lab.* Obtenido de https://www.kaspersky.es/blog/cuatro-ejemplos-de-troyanos-bancarios/1696/

F-Secure. (01 de 05 de 2018). *F-Secure.* Obtenido de https://www.f-secure.com/v-descs/email-worm.shtml

Gaibor, A. V. (12 de 10 de 2007). Utilización de hacking etico para diagnosticar, analizar y mejojrar la seguridad informatica en la intranet. Quito, Pichincha, Ecuador.

Gray, A. (17 de 01 de 2018). *World Economic Forum*. Obtenido de https://es.weforum.org/agenda/2018/01/estos-son-los-mayores-riesgos-que-enfrenta-el-mundo/

Ibáñez, J. M. (19 de 07 de 2015). *Informatica y seguridad en internet*. Obtenido de https://informaticayseguridad.blogspot.com/2015_07_19_archive.html

informáticos, C. d. (20 de 03 de 2017). *CGII.* Obtenido de https://www.cgii.gob.bo/es/publicaciones/prevencion-y-contramedidas-mail-spoofing

Internauta, O. d. (11 de 04 de 2014). *Oficina de Seguridad del Internauta.* Obtenido de https://www.osi.es/es/actualidad/blog/2014/04/11/aprendiendo-identificar-los-10-phishing-mas-utilizados-por-ciberdelincuen

J.M.S. (05 de 03 de 2013). *ABC Redes*. Obtenido de https://www.abc.es/tecnologia/redes/20130305/abci-correos-hackeo-urdangarin-201303051251.html

Joseph C. Chen, Y. Z. (27 de 07 de 2016). *Trend MICRO*. Obtenido de http://blog.trendmicro.es/?p=3039

Mendoza, M. Á. (15 de 09 de 2015). *welivesecurity ESET*. Obtenido de https://www.welivesecurity.com/la-es/2015/09/15/caso-phishing-afecta-usuarios-santander/

Morelli, O. (18 de 03 de 2016). *Los Virus.* Obtenido de https://losvirus.es/adware/

Nacional, A. (2014). *Código Orgánico Penal.* Montecristi.

Panda. (01 de 05 de 2007). *Panda.* Obtenido de https://www.pandasecurity.com/spain/homeusers/security-info/classic-malware/worm/

POLICÍA NACIONAL DEL ECUADOR. (27 de 06 de 2018). *Delitos informáticos o ciberdelitos*. Obtenido de http://www.policiaecuador.gob.ec/delitos-informaticos-o-ciberdelitos/: https://www.elconfidencial.com/tecnologia/2017-06-27/ransomware-que-es-protegerse-claves-ciberataque_1405982/

Portaltic. (16 de 08 de 2018). *Portaltic.* Obtenido de https://www.europapress.es/portaltic/ciberseguridad/noticia-detectan-oleada-correos-electronicos-dirigidos-contra-mas-400-empresas-industriales-20180816124024.html

Profesorado, I. N. (s.f.). *Instituto Nacional de Tecnologías Educativas y de Formacion del Profesorado*. Obtenido de http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m2/servidor_dns.html

Ramiro, R. (03 de 01 de 2018). *Ciberseguridad.* Obtenido de https://ciberseguridad.blog/algunos-tipos-de-ataques-informaticos/

Rebolledo, R. A. (15 de 08 de 2017). *El Economista.* Obtenido de https://www.eleconomista.com.mx/finanzaspersonales/Phishing-y-otros-5-casos-de-fraudes-bancarios-en-el-2017-20170815-0130.html

RIVERO, M. (01 de 10 de 2016). *Info Spyware.* Obtenido de https://www.infospyware.com/articulos/que-son-los-malwares/

Rivero, M. (3 de 10 de 2018). *Info Spyware.* Obtenido de https://www.infospyware.com/articulos/que-es-el-phishing/

Rubio, C. N. (26 de 01 de 2018). *Zoom Tecnológico*. Obtenido de https://www.zoomtecnologico.com/2018/01/26/ataques-ciberneticos-2018/

STIC. (20 de 02 de 2018). *Universidad de Almería*. Obtenido de http://cms.ual.es/UAL/universidad/serviciosgenerales/stic/servicios/recomendaciones/softwaremalicioso/index.htm

Stories, T. (30 de 10 de 2014). *Trending Stories.* Obtenido de https://www.malware.es/windows-spyware/coolwebsearch/

Tecnología, A. (09 de 10 de 2015). *ABC Tecnología.* Obtenido de https://www.abc.es/tecnologia/redes/20151004/abci-google-gmail-201510022053.html

Tercera, L. (31 de 05 de 2012). *La Tercera.* Obtenido de http://www2.latercera.com/noticia/conoce-la-lista-de-los-10-virus-informaticos-mas-peligrosos-de-la-historia/

TI, D. (07 de 04 de 2011). *Diario TI.* Obtenido de https://diarioti.com/epsilon-sufre-“minima”-fuga-de-datos/29479

Tiempo, R. E. (06 de agosto de 2015). *El Tiempo*. Obtenido de www.eltiempo.com/archivo/documento/MAM-456349

ValorTop. (05 de 11 de 2017). *ValorTop.* Obtenido de http://www.valortop.com/blog/que-significa-spam

wikiHow. (15 de 05 de 2016). *wikiHow*. Obtenido de https://es.wikihow.com/eliminar-un-virus-gusano